2009-03

Current federal identity management and the dynamic signature biometrics option

Zanger, Michael S.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

CURRENT FEDERAL IDENTITY MANAGEMENT AND THE DYNAMIC SIGNATURE BIOMETRICS OPTION

by

Michael S. Zanger

March 2009

Thesis Advisor:	Pat Sankar
Second Reader:	James Ehlert

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2009	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Current Federal Identity Management and the Dynamic Signature Biometrics Option		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Michael S. Zanger,			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES: The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

Although Identity Management (IdM) and Biometrics have been engrained in the business practices of private and commercial organizations for decades, the United States Government (USG) and the Department of Defense (DoD) have only truly started to institute a holistic IdM Enterprise within the last decade. More specifically, the DoD has really sharpened the focus on leveraging biometrics since the beginning of the War on Terror. The operational capability to distinguish Red Forces or Gray Forces from Blue Forces is now a common daily occurrence. Regardless of the theater or Area of Operations, U.S. forces are utilizing biometrics to identify our enemies.

In the next phase of implementing a comprehensive IdM Enterprise, the DoD is crafting new IdM policies, procedures, and systems that will distinguish between various levels of access and security controls among Blue Forces. Blue Force IdM architectures are required by specific USG and DoD policies to enforce standardization in policy and application across all federal agencies to improve and synchronize their business practices. And with many agencies crafting their own version of the future, a basic understanding of current IdM and Biometric requirements, as well as potential biometric resources, is necessary to move forward.

14. SUBJECT TERMS Biometrics, Biometrics Task Force, Dynamic Signature Biometrics, Identity Management, IdM Enterprise			**15. NUMBER OF PAGES** 141
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

CURRENT FEDERAL IDENTITY MANAGEMENT AND THE DYNAMIC SIGNATURE BIOMETRICS OPTION

Michael S. Zanger
Lieutenant Commander, United States Navy
MBA, Cameron University, 2001
B.A. in Political Science, Texas A&M University, 1992

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
March 2009

Author: Michael S. Zanger

Approved by: Pat Sankar
Thesis Advisor

James Ehlert
Second Reader

Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Although Identity Management (IdM) and biometrics have been engrained in the business practices of private and commercial organizations for decades, the United States Government (USG) and the Department of Defense (DoD) have only truly started to institute a holistic IdM Enterprise within the last decade. More specifically, the DoD has really sharpened the focus on leveraging biometrics since the beginning of the War on Terror. The operational capability to distinguish Red Forces or Gray Forces from Blue Forces is now a common daily occurrence. Regardless of the theater or Area of Operations, U.S. forces are utilizing biometrics to identify our enemies.

In the next phase of implementing a comprehensive IdM Enterprise, the DoD is crafting new IdM policies, procedures, and systems that will distinguish between various levels of access and security controls among Blue Forces. Blue Force IdM architectures are required by specific USG and DoD policies to enforce standardization in policy and application across all federal agencies to improve and synchronize their business practices. And with many agencies crafting their own version of the future, a basic understanding of current IdM and biometrics requirements, as well as potential biometric resources, is necessary to move forward.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ABIS	Automated Biometrics Identification System
ASD/NII	Assistant Secretary of Defense (Network and Information Integration)
AT&L	Acquisitions, Technology & Logistics
BAT	Biometrics Automated Toolset
BEST	Biometrics Examination Services Team
BFC	Biometrics Fusion Center
BID	Biometrics Integration Directorate
BTF	Biometrics Task Force
BMO	Biometrics Management Office
BOD	Biometrics Operations Directorate
CAC	Common Access Card
CIO	DoD Chief Information Officer
CJIS	Criminal Justice Information Services
COASTS	Cooperative Operations and Applied Science & Technology Studies
COCOM	Combatant Commanders
CONOP	Concept of Operations
DBIDS	Defense Biometric Identification System,
DCCIS	Defense Cross-Credentialing Identification System
DDB	Director, Defense Biometrics
DDRE	Director, Defense Research and Engineering
DEERS	Defense Enrollment and Eligibility Reporting System
DHS	Department of Homeland Security
DIRNSA	Director National Security Agency
DNVC	Defense National Visitors Center
DNTS	Defense Non-Combatant Evacuation (NEO) Operations Tracking Systems
DoD	Department of Defense
DSB	Defense Science Board

EA	Executive Agent
EBTS	Electronic Biometrics Transmission Specification
HIIDE	Handheld Interagency Identity Detection Equipment
HSPD	Homeland Security Presidential Directives
IA	Information Assurance
IAFIS	Integrated Automated Fingerprint Identification System
ID	Identification
IDS	Information Dominance System
IdM	Identity Management
IP	Information Professional
IPMSCG	Identity Protection and Management Senior Coordinating Group
KST	Known or Suspected Terrorists
LPE	Latent Print Evaluator
MAGTF	Marine Air-Ground Task Force
MEF	Marine Expeditionary Force
MEU	Marine Expeditionary Unit
NCIS	Naval Criminal Investigative Service
NSTC	National Science and Technology Council
OMB	Office of Management and Budget
OSD	Office of the Secretary of Defense
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIP	Personal identity Protection
PIV	Personal Identity Verification
PSA	Principal Staff Assistant
RAPIDS	Real-time Personnel Identification Systems
R&SD	Resources & Support Division
SOP	Standard Operating Procedures
TBCMS	Tactical Biometrics Collection and Matching System
TF	Task Force
TMD	Technical Management Division

TPE	Ten-Print Evaluator
TTIC	Terrorist Threat Integration Center
USD	Under Secretary of Defense
USG	United States Government
USMC	United States Marine Corps
VBSS	Visit, Board, Search, and Seizure

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

On a personal note, I would like to thank my wife Michelle for all the sacrifices she has made, not just during the time I worked on this thesis, but throughout my Naval career. Military wives never get their due appreciation for the innumerable times they are left alone to maintain a home and family. For keeping our family going, I am eternally grateful to her.

Professionally, I want to start by thanking Jim Ehlert for the opportunity to work with his great student-led organization COASTS. As his brainchild, COASTS continuously gives motivated students the opportunity to do more than just research a thesis. COASTS allows students to work together, get their hands dirty out in the field, and really expand the envelope of thesis research. The intent is always about looking to improve the operational capabilities of the DoD, while simultaneously making friends from Sister Services and our Allies. I'd also like to thank Dr. Sankar for being such an excellent Thesis Advisor. His generous nature and sage advice were invaluable. My appreciation also goes out to Dr. Richard Kim, the inventor of the DynaSig Bio-Pen. Dr. Kim introduced me to biometrics in general, and more specifically to behavioral biometrics. Listening to him spurred my interest in biometrics and eventually Identity Management. Another stalwart throughout my extended time at NPS was Glenn Cook. More than just an Academic Advisor, Glenn consistently took extra time out of his day to help on all manner of personal and professional issues. His title does not truly reflect the service he gives to his students and NPS at large. I'd be remiss if I did not thank my Program Manager LCDR Chris Taylor. Chris has been a great advisor who makes everyone feel comfortable stopping by to get answers or just shoot the breeze.

Lastly, since they never get recognized enough, I'd also like to acknowledge NPS's Student Services, Travel Office, and the myriad other student support personnel who do a great job keeping all the students on track. Their expertise is the glue that keeps the NPS ship above water.

THIS PAGE INTENTIONALLY LEFT BLANK

PREFACE

Before being unwittingly thrown into the Naval Postgraduate School, I spent fourteen years honing my professional military skills as a Naval Helicopter Pilot. I flew the slightly aged, but none-the-less potent, SH-60B Seahawk from the flight deck's of the U.S. Navy's newest and oldest surface combatants. I amassed over 2200 flight hours and was individually selected for a prestigious Seahawk Weapons and Tactics Instructor billet. It is the helicopter version of Top Gun for those unfamiliar. Life was good.

Roughly a little over four years ago, the pre-selected path I had been following was soon closed off. My career took an unrecoverable blow that forced me into a degree program at a graduate school I had not chosen. As circumstances sometimes end up, I came to enjoy my degree — Information Technology Management. The degree program was tailored for future *managers* of the DoD Information Technology infrastructure, not *technicians*. Which ended up being good for me, since my previous degrees were non-technical — an MBA and a Bachelor's in Political Science. I enjoyed the program so much that I applied for and received a redesignation out of the Aviation Community and into the Navy's Information Professional (IP) Community. This was the only way to ensure that I would have an opportunity to apply the degree following graduation.

During the second half of my first year, I got involved in a student run and faculty supported organization called Cooperative Operations and Applied Science & Technology Studies (COASTS). The organization allows student volunteers to find opportunities for relevant thesis subjects to be evaluated in mock operational situations in the United States and overseas in Thailand. There are opportunities to get involved in actual operational Fleet testing, but the vast majority of tests are done in a more controlled fashion. In one of my first COASTS meetings, I was introduced to some biometric devices and quickly decided that this could be an area I could spend countless hours researching for a thesis and not get bored.

The original intent of my thesis had been to take an interesting and potentially useful dynamic signature biometric device and test it. I would then take the testing data and compare its effectiveness against some of the more popular biometric devices. Eventually, I came to realize that my signature biometric device — the Bio-Pen by DynaSig — would not necessarily compare evenly against other devices. The vast majority of DoD biometrics revolve around devices meant for application in an operational environment. Taking the Bio-Pen and making a case that it could be a useful 'operational' biometric was inherently flawed.

As I further continued my research into biometrics, I came to understand that biometrics was really just a subset resource for a larger Federal Identity Management (IdM) Enterprise. I also found that there were a lot of redundant instructions and work being done independently, especially among the individual DoD services. This, despite federal and DoD policies that dictated all players use a team concept to develop and integrate biometrics. The lack of cohesion was further verified from other students in a Distance Learning IdM certification curriculum. The other students were a varied group from across federal and DoD organizations working on IdM and biometric issues every day.

I eventually realized that I needed to do a thesis that summarized the current state of federal and DoD IdM. With so many disparate instructions, documents, policies, acquisition papers, and memos detailing how IdM needs to be applied, there was no single understandable resource to explain the 'Whys' behind the 'Whats' of the Federal and DoD IdM Enterprise. Concurrently, I wanted to discuss a potential resource in the growing area of Blue Force IdM and biometrics. Just as a signature device is not suited for most operational applications, other biometrics may not be suited for Blue Force business practices. I hope my small thesis helps other people like me interested in IdM and biometrics, but without any background in either, better understand some of the 'Whys.'

I. IDENTITY MANAGEMENT OVERVIEW

A. INTRODUCTION

> *Identity Management: The combination of systems, rules and procedures that defines an agreement between an individual and organization(s) regarding ownership, utilization and safeguard of personal identity information.*
>
> *National Science and Technology Council Biometrics Glossary*

In order to have an intelligent understanding about the field of Identity Management (IdM) within the U.S. Government (USG) and Department of Defense (DoD), it is necessary to have a working knowledge of the overarching documents, instructions, and reports that dictate the current operational and business process goals. One of the biggest issues in trying to understand the current situation in regards to IdM within the USG and DoD, is that there is no general consensus on the way ahead. Even though IdM has gained a lot of attention and resources since 9/11, the majority of efforts are focused on Known or Suspected Terrorists (KST) and military operations. Little federal attention or resources, until recently, have been allocated for Blue (friendly) Force IdM and internal business practices.

This chapter sets the scene in regards to the high level guidance, wherein present and future decisions will be made concerning the implementation and acquisition of IdM Enterprise and Architecture resources. This chapter will summarize, in as concise a format as possible, the most current significant and influential documents shaping the growing field of Federal IdM, as well as some of the implications derived as a consequence of their enactment. To paraphrase my first Officer in Charge every time I asked him how to complete one of his tasks, “What does the instruction say?”

B. NON-DOD FEDERAL DOCUMENTS

1. Homeland Security Presidential Directives

The events of September 11, 2001, ushered in a profound realization that it was no longer acceptable to slowly migrate towards specific national security requirements and milestones. The ability and need to identify potential and confirmed terrorists worldwide was made a high priority requirement by the President for the newly formed Department of Homeland Security (DHS). Through specific Homeland Security Presidential Directives (HSPD), the President outlined requirements with direct implications in IdM and biometrics throughout the federal government. Some of the most significant HSPDs are detailed below.

a. HSPD 6: Directive on Inte gration and Use of Screening Information to Protect against Terrorism

This early HSPD was released in September 2003 and addressed issues dealing with information on individuals known or suspected to engage in terrorist activities. HSPD 6 was designed for the Secretaries of Homeland Security and State, the Director of Central Intelligence, and the Attorney General. The Directive specifically spells out (in a legal-like vocabulary) two objectives towards the goal of protecting the United Sates against terrorists:

(1) Develop, integrate, and maintain thorough, accurate, and current information about individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism (aka Terrorist Information); and,

(2) Use that information as appropriate and to the full extent permitted by law to support;

(a) Federal, State, local, territorial, tribal, foreign-government, private-sector screening processes; and,

(b) Diplomatic, military, intelligence, law enforcement, immigration, visa, and protective processes (White House, HSPD 6).

Any information gathered by HSPD 6 is directed to be provided to the Terrorist Threat Integration Center (TTIC). Along with the above requirement, the responsible parties are required to report to the Attorney General about possible opportunities in which screening can and cannot be conducted.

b. HSPD 12: Policy for a Common Identification Standard for Federal Employees and Contractors

About a year after HSPD 6 was signed in August 2004, the basic requirement to identify terrorists and their affiliates was expanded. It grew by mandating a USG-wide Identification (ID) Standard to include the protection of federal personnel and facilities from intrusion or attack by terrorists. This far reaching requirement for a federal standard was applied to all federal employees, contractors, and contractor employees. Although HSPD 12 is a mere page long, it is quite simply one of the foundational and most influential documents in regards to IdM requirements throughout the USG and DoD.

Section 1 of HSPD 12 more clearly sets forth the overarching goals by stating,

> *Wide variations in the quality and security of forms of identification used to gain access to secure federal and other facilities where there is potential for terrorist attacks need to be eliminated. Therefore, it is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the federal Government to its employees, contractors, and contractor employees (White House 1).*

The Secretary of Commerce was designated as lead and directed to coordinate the development of a Federal Identity Standard among the Secretaries of State, Defense, and Homeland Security; the Attorney General; as well as the Directors of the Office of Management & Budget and the Office of Science and Technology Policy. In accordance with the timeframe requirements spelled out in HSPD 12, the Federal ID

Standard was to have been promulgated six months after the date of the directive. Federal agencies would then have up to four months, but no more than eight months, to have a program in place that meets the Standard. In February 2005, the Department of Commerce released the Federal Identity Standard through the National Institute of Standards and Technology as the Federal Information Processing Standard Publication 201.

2. Federal Information Processing Standards (FIPS) Publication 201-1

FIPS Publication 201-1 — Personal Identity Verification (PIV) of Federal Employees and Contractors is the direct result of the requirement for a single, federal identification standard as directed by HSPD 12. FIPS 201-1 was released in March 2006 to revise and update FIPS 201 that was originally released by the Department of Commerce on February 25, 2005. The first and only Change Notice to FIPS was released on June 23, 2006, to account for changes in graphics standards on the physical PIV card and changes to a specific type of encoding.

The intended goal of FIPS 201-1 in specifying an Identity Standard for federal agencies was

> *…to achieve appropriate security assurance for the multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to federally controlled government facilities and electronic access to government information systems (Technology iii).*

In an effort to achieve that goal incrementally, FIPS 201-1 is divided into two sections, Personal Identity Verification Part I (PIV-I) and Personal Identity Verification Part I (PIV-II). PIV-I requirements for a common identification form (smart card) were to be met by October 27, 2005, while implementation guidance for architectural systems guidance in PIV-II would be issued at a later date by the Office of Management and Budget (OMB). PIV-I is all of three and half to four pages of the ninety-plus page total document. Its objectives are based on HSPD 12 prerequisites that states the physical identification card produced in accordance with the Identity Standard must meet four security and reliability requirements:

(1) Issued based on sound criteria for verifying an individual employee's identity,

(2) Strongly resistant to identity fraud, tampering, counterfeiting and terrorist exploitation,

(3) Can be rapidly authenticated electronically, and,

(4) Issued only by providers whose reliability has been established by an official accreditation process (Technology iv).

In most cases, a large portion of the federal government already had established forms of PIV cards that enabled a short timeframe to be mandated. Despite these 'mandatory' requirements, FIPS 201-1 gave federal agencies an exception clause to the fourth requirement by later stating agencies could either 'self-accredit' or 'use other accredited issuers' until PIV Section II had been made officially (Technology v). PIV-I continues on to describe the Identification Standard's primary objectives in regards to control, identity spoofing and registration, issuance and maintenance, as well as privacy requirements. Throughout the document, it is reiterated that individual agencies are not being forced into using a single credential type. They are allowed to determine the specific card or cards they wish to use and the level of access authority asserted by the card. Whatever the specific credential form chosen by an agency, however, it must meet all of the criteria spelled out in PIV-I.

PIV-II delves deeper into the technical specifications for a holistic PIV system. It further elaborates on the component specifications and processes that ensure interoperability of PIV cards among federal agencies in regards to access control, authentication, and systems management. A pictorial overview of a generic PIV system is shown below in Figure 1 PIV II is logically divided among three functional components:

(1) ***PIV Front-End Subsys tem***: Included is the physical PIV card, card and biometric readers, personal identification number (PIN) input device;

(2) ***PIV Card Issuance and Management Subsystem*** : Includes components for identity spoofing and registration, card and key issuance and management, and the various repositories and services required as part of the verification infrastructure (e.g., PKI directory, certificate status servers…); and,

(3) ***Access Control Subsystem*** : Includes the physical and logical access control systems, protected resources, and the authorization data (Technology 10).

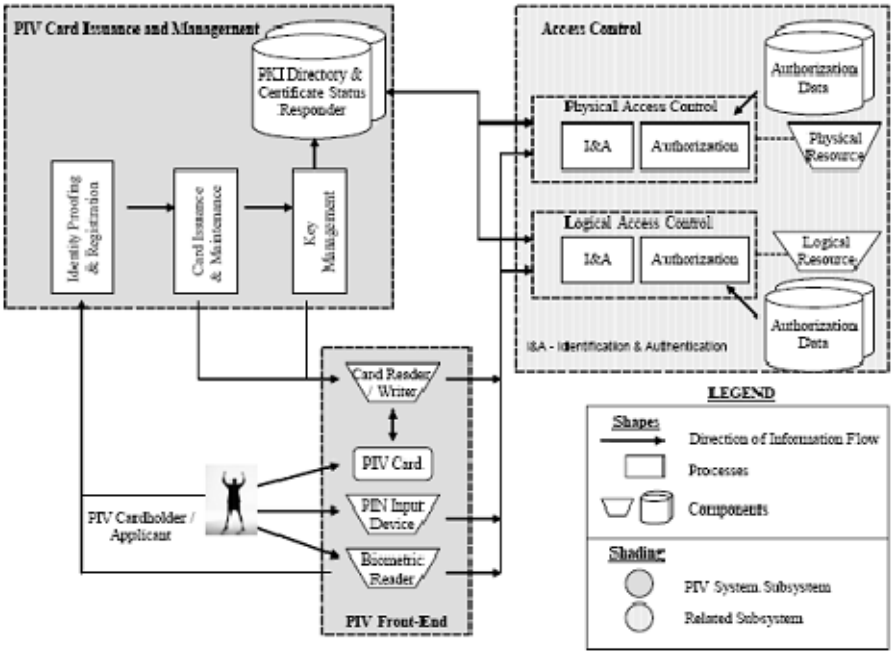


Figure 1. Notional PIV System Model

When the three subsystems of the overall Personal Identity Verification — II architecture are completed by the individual federal departments or agencies, it will ensure secure, homogenous, and adaptable identity management. By conforming to the technical standards of Card Issuance and Management, every federal agency is assured that the individual and the smart card presented for physical or logical access to their resources have been vetted, registered, and approved for appropriate certificate and key

usage. This should be further verified when the individual and their PIV card interact seamlessly with the every agencies' card reader, biometric scanner, or PIN device built to Front-End specifications. And lastly, if the individual mistakenly or surreptitiously attempts to access data or facilities above their authority, logical and physical Access Control subsystems will prevent their efforts and alert the proper authorities as required. A continuous feedback loop within the PIV architecture maintains secure IdM as long as all PIV systems are scrupulously built to the specifications.

Throughout the document, it is consistently reiterated that the need for uniformity and standardization across all federal agencies and departments drives the PIV effort. By standardizing specific physical and logical components among all federal agencies, the enormous benefits derived from economies of scale can be achieved. Agencies are not required to purchase the same hardware or software, but all their hardware and software must be able to interact based on the same language spelled out in FIPS 201-1. When the underlying subsystems of a PIV architecture are able to exchange data through adherence to dedicated standards, federal agencies will no longer waste resources producing multiple identification cards, will decrease the chances for identity fraud with repetitiously stored Personally Identifiable Information (PII), and will increase the level of trust in IdM among agencies.

3. National Science and Technology Council (NSTC) Identity Management Task Force

In the field of IdM and biometrics, the National Science and Technology Council is a very influential organization inside and outside the Executive Office of the President. The Council and its various Committees and Subcommittees are continuously designing the federal IdM and biometrics landscape through coordination, research, and policy recommendations to the President. The website for the National Science and Technology Council (NSTC) has a concise and informative description of the Council and its purpose. It states,

> *The National Science and Technology Council (NSTC) was established by Executive Order (12881) on November 23, 1993 (House). This Cabinet-level Council is the principal means within the executive branch to*

> *coordinate science and technology policy across the diverse entities that make up the federal research and development enterprise. Chaired by the*
>
> *President, the membership of the NSTC is made up of the Vice President, the Director of the Office of Science and Technology Policy, Cabinet Secretaries and, and other White House officials*.
>
> *A primary objective of the NSTC is the establishment of clear national goals for federal science and technology investments in a broad array of areas spanning virtually all the mission areas of the executive branch. The Council prepares research and development strategies that are coordinated across federal agencies to form investment packages aimed at accomplishing multiple national goals. The work of the NSTC is organized under four primary committees: Science, Technology, Environment and Natural Resources and Homeland and National Security. Each of these committees oversees subcommittees and working groups focused on different aspects of science and technology and working to coordinate across the federal government (President).*

Appendix A offers a succinct visual representation of the four committees of the Council, as well as their individual subcommittees. From the brief description of the NSTC, it is slightly misleading as to the membership of the Council. If a formal list of the "Cabinet Secretaries and Agency Heads with significant science and technology responsibilities" were to be listed, the list would cover over two dozen of the U.S. Government's most powerful departments and agencies. The President also has the eternal right to add from time to time "such officials of executive departments or agencies as the President may (House)." In short, this one Executive Order created a Council with an exceptionally large collection of powerful federal officials.

For the purposes of this thesis, the Subcommittee on Biometrics and Identity Management within the NSTC's Committee on Technology deals specifically with the subject material. A pictorial of the Subcommittee on Biometrics and Identity Management's structure is provided below in Figure 2 (Blackburn). The Subcommittee on Biometrics and Identity Management was permanently tasked by the NSTC's Committee on Technology since inception in 2002 to:

a. In Regards to Biometrics

1. Provide technical leadership in the development and implementation of interoperable federal biometrics systems;

2. Develop and implement multi-agency investment strategies that advance biometric sciences to meet public and private needs;

3. Develop and adopt biometric standards as specified in the *NSTC Policy for Enabling the Development, Adoption, and Use of Biometrics Standards*; and,

4. Develop consensus strategic outreach plans for biometrics, including collaboration on www.biometrics.gov, the annual Biometric Consortium Conference and other events.

b. In Regards to Identity Manage ment (of whic h Biometr ics is a Subset)

1. Identify cross-sector IdM issues, and develop and implement plans to address the federal government's priority S&T need;

2. Facilitate the inclusion of privacy-protecting principles in IdM system design;

3. In January 2008, the Promote a scientifically educated and aware public that properly understands IdM technologies, federal programs and issues; and,

4. Strengthen international and public sector partnerships to foster the advancement of IdM technologies (Council, Subcommittee Overview).

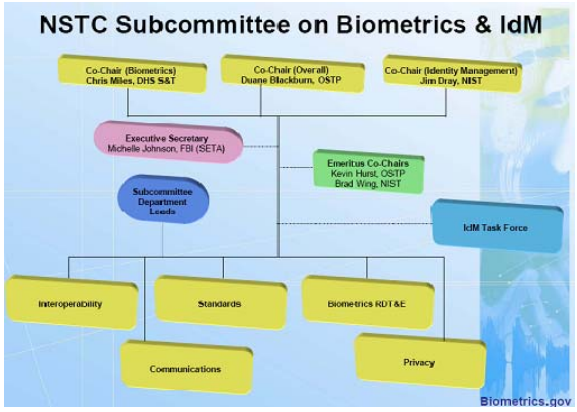


Figure 2. Subcommittee on Biometrics & IdM Structure

Subcommittee for Biometrics and Identity Management was further directed by the NSTC to form a Task Force (TF) on Identity Management. The Task Force lasted for six months and was charged with three primary objectives:

(1) Provide an assessment of the current state of IdM in the U.S. Government;

(2) Develop a vision for how IdM should operate in the future; and,

(3) Develop first-step recommendation on how to advance toward their vision (Council, Identity Management Task Force Report 2008, ES-2).

The Task Force approached the assignment from two different angles realizing they had a limited amount of time to summarize an extremely large subject. A portion of the TF's resources were used to assess publicly available Privacy Impact Assessments (PIA) which spell out the privacy impact of any substantially revised or new Information Technology System (Security). PIAs were first mandated by the E-Government Act of 2002 in recognition that advances in Information Technology also had important ramifications on the protection of personal information contained in government records and systems (Security).

The second approach was to coordinate with the Office of Management and Budget to conduct a survey of the Federal Chief Information Officer's Council. The scope of the survey and TF's overall report tried to address uses of Federal IdM in every possible way internal and external to the federal government, to include between the

federal government and international organizations or commercial entities. Wherever a Federal IdM system could possibly be used or accessed, the TF attempted to evaluate. The TF on Identity Management also used the following definition of Identity Management as part of its methodology to benchmark the concept for those surveyed,

> *The combination of technical systems, rules, and procedures that define the ownership, utilization, and safeguard of personal identity information. The primary goal of the Identity Management process is to assign attributes to a digital identity and to connect that identity to an individual (Council, Identity Management Task Force Report 2008, ES-1).*

Some of the big picture findings from the combined efforts were that there are more than 3000 IdM-related systems within just the federal government that utilize some form of Personally Identifiable Information (PII)[1]. Remember, this does not include *any* non-federal systems that may interact with USG systems. Not surprisingly, the preponderance of these systems were designed, utilized, and managed in their own independent 'stovepipes.' Another finding from the TF's efforts was the lack of an agreed-upon definition for "Identity Management." It's not difficult to see how disparate IdM systems are so incompatible when there is no aggreement on a common definition of IdM. Among the more than 3,000 systems, roughly only fifteen percent collect or use biometrics, security questions, or tokens (Dray). PINs, login aliases, passwords, date of birth, and Social Security numbers are the most common forms of IdM information collected (Dray).

The major consequences noted from this lack of a Federal IdM Enterprise are

(1) Duplicative identity data is often stored in multiple locations within the same agency, as well as across agencies, causing a negative impact on accuracy and complicating an individual's attempt at redress;

[1] Personally Identifiable Information (PII) is defined by the NTSC as "[t]he information pertaining to any person which makes it possible to identify such individual (including the information capable of identifying a person when combined with other information even if the information does not clearly identify the person)". This may be interpreted as "any information which identifies a person to any degree".

(2) A lack of commonly used standards makes appropriate cross-function collaboration difficult, thus impacting both time-sensitive mission needs as well as reducing personal privacy;

(3) Privacy protection efforts vary in complexity across agencies; and,

(4) There is no single government-wide forum responsible for coordinating and homogenizing IdM efforts across the U.S. government (Council, Identity Management Task Force Report 2008, ES-3).

The Task Force on Identity Management concurrently identified four major opportunities that could systematically demonstrate a return on investment. The first was the ability to capitalize on existing investments in digital infrastructure. Through the previously discussed FIPS 201, the federal government has established technical standards to create basic identifications for employees. Even though there is currently not a robust Federal IdM infrastructure to support the full utilization of these ID's, the common FIPS 201 standard enables the prospect for design and implementation of FIPS capable systems throughout the USG (Council, Identity Management Task Force Report 2008, 14).

The second opportunity the TF identified for a Federal IdM Enterprise was the ability to achieve multiple efficiencies in design and use (Council, Identity Management Task Force Report 2008, 15). Because there is an enormous amount of repetitive data residing on literally thousands of disparate systems, a federated IdM architecture would alleviate this redundant waste. Surplus and cumulatively expensive resources storing and managing the same data would be eliminated. Centralized data would be more easily updated and available to all systems under proper access controls. And most importantly, the chances for compromised data would be dramatically decreased because there would be limited access to a single secured repository of data, and there would be auditing mechanisms enabling the ability to more quickly determine breaches or violations of integrity.

Third, the data management standards and policies of separate architectures would be harmonized through standardization (Council, Identity Management Task Force Report 2008, 15). The resources and policies of every Federal IdM system would be built upon the same foundation of hardware, software, and policy standards. This would allow each agency or organization the flexibility to acquire the systems that work best for them, AND be interoperable with the systems of every other agency. And lastly, the standardization of IdM systems would allow for a true single sign-on access across multiple systems (Council, Identity Management Task Force Report 2008, 15). There would no longer be a need to continuously remember or write-down PIN's or passwords for each and every system. This in turn would reduce potential security risks. If every system operated under the same standards and guidelines, every system would accept any vetted individual's access authority by near or instantaneous verification of credentials.

The data and findings gathered by the Subcommittee on Biometrics and Identity Management's Task Force on Identity Management will be used to craft the vision for a federated approach to a Federal IdM Enterprise. To this end, the Task Forces' seven top-level goals follow:

(1) Configuration and operation of a "network of networks" to securely manage digital identities, based on a set of common data elements for stored PII that will allow it to be leveraged by a broad range of applications;

(2) Security of process, data transmission, and storage; this includes and embraces all features of confidentiality, integrity, authenticity, and privacy, including use of encryption and multifactor authentication;

(3) Auditability of processes, with complete, automatic, and secure record keeping;

(4) Ubiquitous availability, at global distances, of strong verification of stored digital identity when called for or needed to support an authorized application;

(5) Standards-based connectivity, interoperability, and extensibility of supporting IT architecture;

(6) Preservation of application-specific PII data under control of application sponsors, with minimal exposure to unauthorized access or unnecessary transmission across networks; and,

(7) Ability of prospective application sponsors to develop, install, and operate applications in a way that permits the supporting IT grid to be seen as a freely available, ubiquitous service (Council, Identity Management Task Force Report 2008, ES-5).

C. DEPARTMENT OF DEFENSE DOCUMENTS

1. Overview

IdM as a business and operational construct is relatively new to the Department of Defense. The applications and hardware for biometrics have been more heavily developed as a result of the War on Terror, but it has only been understood in the last few years that biometrics is actually just a subset of a larger IdM vision. As a result, the DoD does not have any formal IdM Enterprise instructions to date. They are either currently in development or have appeared as conceptual statements in other documents. Through research, there are references to documents like the ***DoD Roadmap to Identity Superiority*** and the ***DoD Identity Protection and Management Vision*** in some GAO reports and other DoD high-level documents.[2] For whatever the reasons, these documents do not appear on any DoD or reference websites. It is possible they never made it to a final approved draft or the vision is still uncertain. The fact that the DoD does not have concrete guidance for an IdM Enterprise or Architecture speaks volumes to the DoD's current lack of IdM focus. The following documents are the closest to approved and accessible guidance for specific aspects of DoD IdM.

[2] As an example, a September 2008 GAO Report titled *DEFENSE MANAGEMENT: DOD Needs to Establish Clear Goals and Objectives, Guidance, and a Designated Budget to Manage Its Biometrics Activities* states",…in September 2006, the (DOD CIO's) Identity Protection and Management Senior Coordinating Group produced a draft *Roadmap to Identity Superiority*. This document provides a more specific strategic vision of biometrics and some associated programs, including specific goals and expected timelines. However, DOD officials told us that the document has not been finalized.

2. Deputy Secretary of Defense Directive-Type Memorandum (DTM) 08-006: "DoD Implementation of Homeland Security Presidential Directive — 12 (HSPD-12)"

The three-page memo (six pages total with an attachment on responsibilities) released 26 November 2008 stated that it immediately establishes a DoD policy for the implementation of Personal Identity Verification Section I. As previously discussed, PIV I details the implementation of a smart card for all DoD employees, contractors, and employees of contractors who request or have a need to access DoD facilities and resources. The memo, however, does not mention anywhere about policy pertaining to PIV Section II, or the larger Personal Identity Verification Architecture. The memo also states that it should be replaced by a formal DoD Instruction within 180 days (Defense).

In order to meet the requirements of Homeland Security Presidential Directive - 12, the DoD' Common Access Card (CAC) will be the official identity credential and be accepted by all DoD Components. The CAC can be used for logical or physical access to DoD facilities and resources. Although the CAC is to be the accepted DoD identity credential, it will be at the discretion of individual federal facilities and information systems managers to grant or deny access. Furthermore, upgrades to the current Real-time Personnel Identification Systems (RAPIDS) will be made to ensure that the CAC and CAC issuance process fully complies with HSPD-12. This progression is expected to occur over the next four years as current CAC's expire and RAPIDS receives the necessary upgrades (Defense).

3. Department of Defense Directive (DoDD) 1000.25

DoDD 1000.25 — DoD Personnel Identity Protection (PIP) Program was originally promulgated in July 2004, but was updated in April 2007. This directive cancels and replaces three previous DoD Directives and Instructions relating to military and civilian IDs, as well as the Defense Enrollment and Eligibility Reporting System (DEERS). Its purpose as stated,

> *The PIP shall be the Department of Defense's program for: addressing threats to the individual personal privacy of its Members, employees, and beneficiaries; establishing a secure and authoritative process for the*

> *issuance and use of identity credentials on the Department of Defense; and ensuring that DoD benefits and access to DoD physical and logical assets are granted on authenticated and secure identity information. (USD (P&R))*

Although not specifically an IdM instruction, DoDD 1000.25 works hand-in-hand anywhere HSPD-12 and the DoD's Common Access Card are applicable. As such, it appears and reappears in a multitude of DoD and Service instructions, directives, and policy statements of varying importance. The PIP program influences all of the following systems that operate within the sphere of identity implementation and operations: DEERS, RAPIDS, Defense Biometric Identification System (DBIDS), Defense Cross-Credentialing Identification System (DCCIS), Defense National Visitors Center (DNVC), and the Defense Non-Combatant Evacuation (NEO) Operations Tracking Systems (DNTS) (USD (P&R)).

Oversight of the PIP Program is delegated to the Identity Protection and Management Senior Coordinating Group (IPMSCG) under the Assistant Secretary of Defense (Network and Information Integration) (ASD/NII) and DoD Chief Information Officer (CIO) (USD (P&R)). The IPMSCG must ensure that the PIP Program is ready to add additional capabilities and systems as technologies emerge in the future. In essence, the PIP Program is a scaled-version of an IdM Architecture that seeks to implement and leverage standardization of identity credentialing and processing across the varying DoD identity systems.

II. BIOMETRICS OVERVIEW

A. INTRODUCTION

> *Biometrics: As a characteristic: A measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition.*
>
> *As a process: Automated methods of recognizing a biometric subject based on measurable biological (anatomical and physiological) and behavioral characteristics.*
>
> ð National Science and Technology Council Biometrics Glossary

As with the field of Identity Management, biometrics in the USG and DoD is in a state of controlled chaos. Biometrics, however, is far more advanced in operational application, business use, and policy formation. Referencing Appendix B will give an appreciation for the language that has already evolved around the subject. There are a lot of initiatives and programs with only limited coordination between them, whether it is a Special Operations Unit taking multi-modal biometrics into the mountains of Afghanistan or a diligent TSA employee verifying the biometrics of a foreign traveler coming into the United States. Resources are being wasted through duplication of efforts, a lack of interconnectedness among databases, and an inability of most IdM or biometrics systems to simply exchange or verify data with another system even if connected.

For a long time, biometrics was seen as a separate resource in identifying Red or Gray forces, and occasionally Blue forces. As resources for and the actual application of biometrics expanded after 9/11, biometrics was better understood to be a component of the wider field of Identity Management. Initial versions of federal IdM architectures or enterprises began to take shape, and biometrics became the tool by which better information and intelligence could be gathered and shared. This chapter summarizes and quotes from the latest iterations of both federal and DoD documents that describe how biometrics is expected to be applied currently and in the future. Most documents are

relatively new by DoD standards, and account for the information on biometrics already acquired and the acceptance that biometrics is no longer a separate field. In regards to how biometrics is specifically employed on a daily basis, this topic will be more thoroughly handled in the next chapter.

B. NON-DOD FEDERAL INSTRUCTIONS

As a tool in the implementation of a Federal IdM Enterprise, the use and application of biometrics has truly gained momentum. Despite the fact that commercial businesses and organizations have been using biometrics for decades, the USG and DoD have only become serious about the implementation of biometrics since the Global War on Terror began at the end of 2001. Even then, the vast majority of applications that took advantage of the benefits of biometrics were operational systems used to distinguish Red and Gray forces from Blue Forces, but not among varying grades of Blue Forces.

Over the last few years, however, a drive and accompanying resources have been applied towards evaluating biometrics systems for business and operational systems that distinguish Blue Forces from other Blue Forces. From a general business perspective, the greatest security threat is still the Insider Threat. There is a specific and quantifiable need to distinguish people by access to facilities, privileges to applications, or basic security levels. In the federal government and DoD, one only has to do a quick search on Google or any news source to find plentiful examples of Personally Identifiable Information (PII) that was randomly lost or stolen by federal and DoD employees. Laptops with little or no security features installed and enabled continue to disappear or remain unaccounted for that potentially disclose the private medical, social security, and personal information of hundreds of thousands of active duty military, retirees, and civil servants. This problem grows exponentially when you realize that only recently have security standards been enacted that each federal agency or organization is held accountable to meeting. Dig deeper and these issues multiply again after the realization that divisions and departments within individual agencies do not always use a single standard, and often do not even effectively attempt to coordinate their efforts.

1. HSPD 24 and National Security Presidential Directive 56: Biometrics for Identification and Screening to Enhance National Security

HSPD 24 is a very recent directive in the larger vision for biometrics with a publication date of June 5, 2008 (White House, Homeland Security Presidential Directive 24). The Directive instructed the Attorney General to have a plan of action within 90 days that has been coordinated with the Secretaries of State, Defense, and Homeland Security, the Director of National Intelligence, and the Director of the Office of Science and Technology Policy. Following the submittal of the plan, all of the responsible parties would have a year to submit a report outlining their implementation of the directive, an action plan, and any additional actions required for implementation.

Although HSPD 24 does not specifically address the use of biometrics for Blue Force identification and screening, HSPD 24 does seek to unify the efforts of federal agencies in regards to the collection, use, and sharing of terrorist biometric data. Specifically, HSPD 24 states,

> *Many agencies already collect biographical and biometric information in their identification and screening processes. With improvements in biometric technologies, and in light of its demonstrated value as a tool to protect national security, it is important to ensure agencies use compatible methods and procedures in the collection, storage, use, analysis, and sharing of biometric information (White House, Homeland Security Presidential Directive 24).*

Furthermore, HSPD 24 gives more explicit direct direction on how to achieve the goal.

> *Through integrated processes and interoperable systems, agencies shall, to the fullest extent permitted by law, make available to other agencies all biometric and associated biographical and contextual information associated with persons for whom there is an articulable and reasonable basis for suspicion that they pose a threat to national security (White House, Homeland Security Presidential Directive 24).*

Interestingly, the definition chosen for use only covers the characteristic portion of biometrics. It does not mention the second half of biometrics as a process like written in the NSTC version in Appendix B. As a process, "biometrics" is defined as automated

methods of recognizing a biometric subject based on measurable biological (anatomical and physiological) and behavioral characteristics. With the stated intention of this directive to force federal agencies to work together, it would have been prudent to also emphasize the process half of biometrics to the intended audience.

2. The National Biometrics Challenge

In August 2006, the National Science and Technology Council's Subcommittee on Biometrics (now called the Subcommittee on Biometrics and Identity Management) published a report titled "The National Biometrics Challenge." The intent of this report was to lay out a common agenda of challenges and opportunities for the 'biometrics community' — government, industry, and academia. In developing this report and its attending multiple lists, the NSTC Subcommittee on Biometrics analyzed the distinctiveness of biometrics as an identification tool, market and social forces influencing biometric applications, and requirements for future capabilities (Biomtrics 1). Although the use of biometrics is becoming more commonplace, applications are usually stovepiped and disconnected. Current security and business requirements are dictating highly interconnected biometric systems to rapidly ID personnel across any operational environment.

As a capability in the larger architecture of IdM, biometrics has some distinct advantages over other identity processes. Biometrics is currently the best available real-time capability for identifying personnel. Secondly, the direct attachment of biometrics to an individual allows it to be integrated and layered with other security or verification resources. Third, biometrics that are scalable and interoperable facilitate the identification of repetitive biometric data across the enterprise. Lastly, biometrics are difficult, though not impossible, to copy or compromise because they are tied to a specific individual's characteristics — physiological and behavioral. Overall, the calculable benefits of bioimetrics when applied in a holistic enterprise architecture are valuable resources saved by eliminating redundant data, increased effectiveness through shared data, and improved security by layering and overlapping applications (Biometrics 4).

Following all their research, the Subcommittee on Biometrics narrowed the influences driving the evolution of biometrics into the following four primary forces:

1. National Security.
2. Homeland security and law enforcement.
3. Enterprise and e-government services.
4. Personal information and business transactions.

There were also a collection of specific needs identified across each of the four primary forces. One of those was the need to accurately ID individuals in real-time in order to distiguish threats from unknowns or friendly forces. In order to do this, the Subcommittee identified the need for accurate, rugged, multi-modal biometrics that rely on standards that imporve interoperability across agencies. Another need was enterprise and e-government services which streamline and secure recognition to create 'federated identities' across organizational boundaries and ensure privacy standards. A third requirement was personal and business transaction solutions that decrease identity theft in cost-effictive and user intuitive ways.

Four prominent challenges were then identified as the most significant in regards to the primary forces:

1. Improve collection devices (biometrics sensors).
2. Develop more efficient and effective large-scale operational capabilities (biometrics systems).
3. Establish standards for plug-and-play performance (biometrics systems interoperability).
4. Enable informed debate on why, how, and when biometrics should and can be used (biometrics communications and privacy) (Biomtrics 2).

These four challenges cut across all four of the previously mentioned primary forces to one degree or another.

If the required needs already discussed could be filled, there would be substantial benefits to be gained across both the public and private sectors. When the biometric sensors are designed and produced to specifications, real-time biometric data could be transmitted in almost any environment to support law enforcement, military, or homeland security positive identifications of KSTs or foreign visitors. Systems could lose or change out sensors without any degradations. Biometric architectures in a standards driven environment would no longer be hamstrung to specific vendors. Confidence by both owners and customers would increase even as biometrics systems scale up to enterprise levels. Biometric data would be consistent across the enterprise without wasteful duplication as biometric systems reach real interoperability. Lastly, informed debate about the application of biometrics and the societal implications would demystify the technology and improve overall cooperation (Biomtrics 13-16).

C. DEPARTMENT OF DEFENSE INSTRUCTIONS

1. Department of Defense Directive (DoDD) 8521.01E: Department of Defense Biometrics

DODD 8521.01E was released in February 2008 by then Deputy Secretary of Defense Gordon England. Like most DoD directives, it stated in clear terms who had been designated to which position and what their specific responsibilities were to be. The major significance of this document is that it consolidated numerous previous biometrics and related instructions, as well as making slight adjustments to the DoD biometrics chain of command. Under this instruction, the DoD Biometrics Principal Staff Assistant is the Director, Defense Research & Engineering under the Under Secretary of Defense for Acquisition, Technology and Logistics. Whereas the Secretary of the Army had previously been designated the DoD Executive Agent (EA) for just integration of biometrics technologies, the Secretary was now designated EA for *all* DoD biometrics (Defense, Department of Defense Biometrics).

In order to establish a common language for discussing biometrics, this DoD instruction notes that it is using the NSTC Subcommittee on Biometrics Glossary (Appendix B of this thesis). This will help ensure that both military and civilians alike

can understand one another when talking and writing about biometrics. The Policy section of the Directive reiterates a lot of previously mentioned requirements such as the requirement to improve efficiency and effectiveness, eliminate redundant efforts, coordinate through the EA to leverage current acquisitions, develop systems for interoperability, develop continuity of operations for contingencies, and that all biometrics data shall be maintained and controlled by the DoD. Under the Responsibilities section, the requirement to ensure that DoD meets all the requirements of HSPD 12 fall to the Under Secretary of Defense for Personnel and Readiness. The Under Secretary also has the major task for ensuring all policies and procedures for IdM and ID protection meet current DoD biometric capabilities and standards. A significant responsibility when noted that the area of DoD Blue Force biometrics is where significant resources and thought are shifting towards. More specific details about how the Secretary of the Army as EA for Biometrics is concretely applying his responsibilities in operational biometrics is found next in Chapter III on the Biometrics Task Force.

2. Report of the Defense Science Board Task Force on Defense Biometrics

In April 2006, the Under Secretary of Defense (USD) for Acquisition, Technology, and Logistics (AT&L) requested the formation of a Task Force on Defense Biometrics from the Defense Science Board (DSB). The USD (AT&L) stated that the Department of Defense was working in an ad hoc and reactive fashion to the ever increasing demands for biometrics and IdM technologies. The DoD was still operating under a pre-9/11 mindset defined by pre-9/11 guidance (TF on Biometrics 93). The official USD (AT&L) memorandum required interim results by May 2006 and a final report by November 2006. Research was completed in September 2006 by the DSB Task Force on Biometrics, and the final report presented to the USD (AT&L) in March 2007.

One of the first points made in the Report's Executive Summary was the TF's summary conclusion that the real topic was the DoD's IdM posture, not just current biometrics capabilities. Biometrics is an important technology in the larger DoD IdM

Enterprise, but still just one piece of the overall IdM puzzle. The theme driven home is that biometrics is but one means towards a holistic IdM Enterprise. The TF of Defense Biometrics then identified six top level interim findings summarized below:

1. The importance of identity management and the role of biometrics in the Department of Defense are underappreciated.

2. The present management structure largely reflects pre-9/11 requirements: a "blue" focus inside DoD, and conceived in the context of information assurance.

3. Urgent battlefield needs are not being met. The current "program" appears to lack the necessary warfighter customer orientation.

4. Requirements will continue to grow as current business processes scale up, as new applications come on line, as the adversaries adapt and as new threats emerge.

5. Technology is changing for the better. New technologies must be inserted rapidly.

6. There appears to be considerable benefit in a Department-wide authority for identity management and biometrics, accountable and responsible for its funding, policy, vision and direction, and sustainment (TF on Biometrics 3).

The DSB TF on Defense Biometrics Report elaborated on DoD issues with biometrics in both technological and organizational contexts. In both contexts, the Report intentionally and continuously related the issues and material back to how they should support broader DoD IdM processes. When the Report elaborated on the general role of biometrics, it stated that biometric processes themselves "offer the high assurance of uniqueness in initial registration, and added confidence to ID assertion" (TF on Biometrics 15). The TF also concluded that any ID related processes cannot be accurate without biometrics, because it is necessary to positively link an individual asserting an identity to a historical digital biometric instance of the individual. Another point made in the TF Report was that the initial introduction of biometrics to the public after 9/11 created a sense of mistrust and misunderstanding because the government failed to clearly and adequately explain what was being done and why. More recently, the public has cautiously accepted biometrics as they have become more educated about the

technology and more accustomed through exposure. Lastly, the perfromance measurements of biometrics have moved beyond the inflated rhetoric of original gradiose expectations to realistic probabilities of potential applications (TF on Biometrics 15).

A three category system for identifying personnel or resources, that is referred to as the Identification Trinity, is described by the Report. The three categories that make up the ID Trinity are: (1) something you have, (2) something you know, and (3) something you are. The strength of the authentication increases when ID processes use two or all of the categories in combination to make a positive ID. The most common form of ID has, and continues to be, something an individual has. Examples like a birth certificate or drivers license are the mainstay of attempting to prove one's identity. These physical objects are commonly referred to as tokens in the IdM lexicon[3]. Something you know is also a very commonly used identifier. Examples of these include passwords, PINs, or answers to pass phrases. Authenticators from this category are easy to produce, but also easily compormised through social engineering or simple laziness. The third category of something you are comprises the physical and behavioral features that most uniquely identify one individual from another. These features do not need to be memorized, are harder to duplicate, and harder to deny during an authentication process. Biometrics is this third category.

When the TF on Defense Biometrics completed their research, they generated forty-six recommendations broken down into six categories: Information Management and Information Sharing Issues; R&D, Materiel and Technology Issues; Issues Beyond the Department of Defense; Issues Within the Department of Defense; DoD Organizational Issues; and, Legal and Privacy Issues. The most relevant recommendations dealing directly with biometrics and the application of biometrics are:

3 As previously mentioned, HSPD -12 outlines the requirements for a strong common identity credential (or token). The DoD Common Access Card currently used meets HSPD-12 requirements for a FIPS-201 compliant token.

a. Information Management and Information Sharing Issues

Recommendation 19: The OSD PSA for Biometrics, with the ASD/NII, should ensure that scalability issues are addressed specifically in anticipation of scaling key identity management systems and processes globally.

Recommendation 42: That the PSA for Biometrics cause the issue of using the biometric, itself, for remote authentication across a broad multi-use network to be re-examined. Participants in the re-evaluation would include, inter alia, the CIOs, the ASD (NII), and the DIRNSA (TF on Biometrics 86).

b. R&D, Materiel and Technology Issues

Recommendation 3: The PSA for Biometrics should undertake to develop field-deployable DNA collection and matching equipment that requires less skill to achieve operationally worthy results, and the data architecture for accessing repositories for match should be designed and deployed apace. Additionally, the PSA, in coordinate with appropriate authorities, should investigate options related to organizational, physical and/or data collocation with other/larger elements of the total DoD biometrics/IM enterprise.

Recommendation 6: Conduct research focused on defining, verifying, quantifying and improving biometrics collection/matching performance in multi-modal systems. Evaluate alternative methods for comparing and weighting results of matching algorithms of different biometric modalities within a single system; seek to establish optimal mixes/combinations of modalities in various applications and scenarios. Examine issues specifically related to multi-modal data storage and system architecture.

Recommendation 8: Support research efforts by DARPA and others into extended-range human biometric identifiability and tracking. Explore feasibility of "unattended surveillance" of larger areas. Examine applicability of biometrically-based capability for long-range identity assertion in operational scenarios.

Recommendation 10: Quantify, operationalize, and improve upon 3D as a basic biometric modality. Explore development of coherent, bi-static 3D imagery collection capability, with cameras separated over some distance. Conduct an ongoing, basic-research effort in biometrics, seeking to discover new modalities, and previously-unknown insights from existing collection and operational biometrics. Seek to identify and operationalize promising new areas of biometrics application, appropriately.

Recommendation 14: Support multi-agency research to identify and refine possible new biometric modalities related to residual/latent information (TF on Biometrics 87-88).

c. Issues beyond the Department of Defense

Recommendation 24: The OSD PSA for Biometrics should establish the policy and technology basis for associating biometrics with the broader field of Identity Management in the whole range of DoD applications and requirements, and support interagency efforts to do the same.

d. Issues within the Department of Defense

Recommendation 36: The OSD PSA should work with USD/P&R to establish an "Identity Management Community" within the DoD, to establish, support and manage a career-long continuum of training, education and professional development in this field.

Recommendation 38: The OSD PSA for Biometrics, in coordination with and supported by the USD/P&R, should examine the model used to support and encourage the emergence of Information Assurance (IA) as a recognized and accredited academic discipline in the 1990s, in terms of its possible relevance for reproduction and application to IM/biometrics.

Recommendation 46: The OSD PSA for Biometrics, in coordination with appropriate authorities, should seek the creation of comprehensive security policy or policies for biometrics. Such policy should embrace all phases of developmental and operational use, and all other relevant considerations.

e. DoD Organizational Issues

**Note: Recommendations in this section are repeated in other categories.

f. Legal and Privacy Issues

Recommendation 40: The Department of Defense, if not the USG, must seek to engage responsible advocates of privacy early in the design and application of identity management systems; the serious purpose of the system must be communicated and understood; and, the data must be limited to that purpose.

Recommendation 41: The OSD PSA for Biometrics should request a broad review by the Office of General Counsel (OGC) of the privacy implications of biometrics use within the Department, which should be coordinated with the Department of Justice. Based on the results the PSA, in coordination with the Defense Privacy Board and the OGC, should create comprehensive biometrics privacy policies and strategies as required to support the range of defense missions, consonant with interagency efforts (TF on Biometrics 86-92).

Department of Defense involvement in the shaping of policy and doctrine was expressed in the Report with the understanding that it was no longer possible to operate in a vacuum. Higher level directives like HSPD-12 mandated that the DoD become actively involved with other governmental agencies, inter-governmental agencies, international agencies or allies, and the commercial sector. The DoD is inextricably linked with all of these entities and has too much at stake to not try to direct the activities of all the constituencies in evaluating biometric or IdM policy and doctrine. For example, the DoD shares and exchanges biometric data with the FBI through the FBI's IAFIS database. Likewise, the DoD shares its biometric information with other federal departments like the Department of Homeland Security. In order to achieve true

global capabilities, the DoD must leverage its relationships to maximize interoperability, standardization, and economies of scale. Most importantly, the DoD needs to become an active stakeholder to ensure that international policies and technologies remain favorable to U.S. security priorities (TF on Biometrics 60).

The TF ends the report by relating the importance of biometrics in identification and verification to the process of personnel security. Government agencies and departments expend a lot of resources to properly vett personnel attempting to attain security clearances. These clearances will then be used to protect our nation's most important security information and systems. Without tying a biometric to the individual investigated and possibly polygraphed, it is still possible for that person to fake their identity. When understood from this perspective, biometrics would clearly add a much higher level of identity assurance when used to identify govenrment contractors or new recruits as it would throughout the personnel security process.

THIS PAGE INTENTIONALLY LEFT BLANK

III. CURRENT DOD BIOMETRICS OPERATIONS: THE BIOMETRICS TASK FORCE

A. INTRODUCTION

In this chapter, a detailed overview of the operational component of the Biometrics Task Force (BTF)—Biometrics Operations Directorate located in Clarksburg, West Virginia is explored. If someone wants to know what the Department of Defense is doing on a daily basis in regards to operational IdM, one of the best places to start is the Biometrics Task Force Formerly known as the Biometrics Fusion Center, this specific facility is now referred to as the Biometrics Task Force — West. The Plans and Policy component of the BTF, generally referred to as BTF — East, is located in Crystal City, VA. Details and information about BTF operations were gathered from a personal tour of the facilities on December 16, 2008 and from the Unclassified materials supplied by the BTF — West personnel.[4]

B. BACKGROUND & COMMAND STRUCTURE

1. Background

Following a study commissioned by Congress in 1999, it was determined that biometrics was an emerging technology that would have a significant impact on Department of Defense operations. As such, the use of biometric technologies needed to be coordinated, standardized, and funded. The Biometrics Management Office (BMO) was established in 2000 under the Army's Chief Information Officer (CIO) with the Secretary of the Army as the Executive Agent for the DoD. This action made the BMO the epicenter for all things biometrics in and among all the services and DoD agencies.

[4] Specifically, I was able to coordinate the tour through Theresa Marinaro, BTF-W Office Assistant. My knowledgeable tour guide and general BTF representative was David Phares, Senior Project Manager with Computer Sciences Corporation (CSC). The following people also generously made themselves available to answer my litany of questions during the tour: Kim Quinn of I3 — Deputy Operations Manager, DoD Enterprise Systems; Lauren — Ten Print / Latent Print Evaluator Supervisor; plus Karla Buckel and Robert Peters — Hardware Test Engineers also with CSC.

BMO focused primarily on Information Assurance (IA), specifically network access, but has iteratively broadened its scope as technology and operational requirements have evolved (Biometrics Task Force).

Figure 3 below shows the most current chain of command for both BTF East and West. The Secretary of the Army is Executive Agent (EA) who further delineated the Army G-3 as its acting EA. The Secretary as Executive Agent reports to the Principal Staff Assistant (PSA) — Director, Defense Research and Engineering (DDRE) — Director, Defense Biometrics (DDB). Figure 3 also demonstrates the myriad of military and interagency relationships focused on biometrics within the DoD and U.S. Government (Lohman).

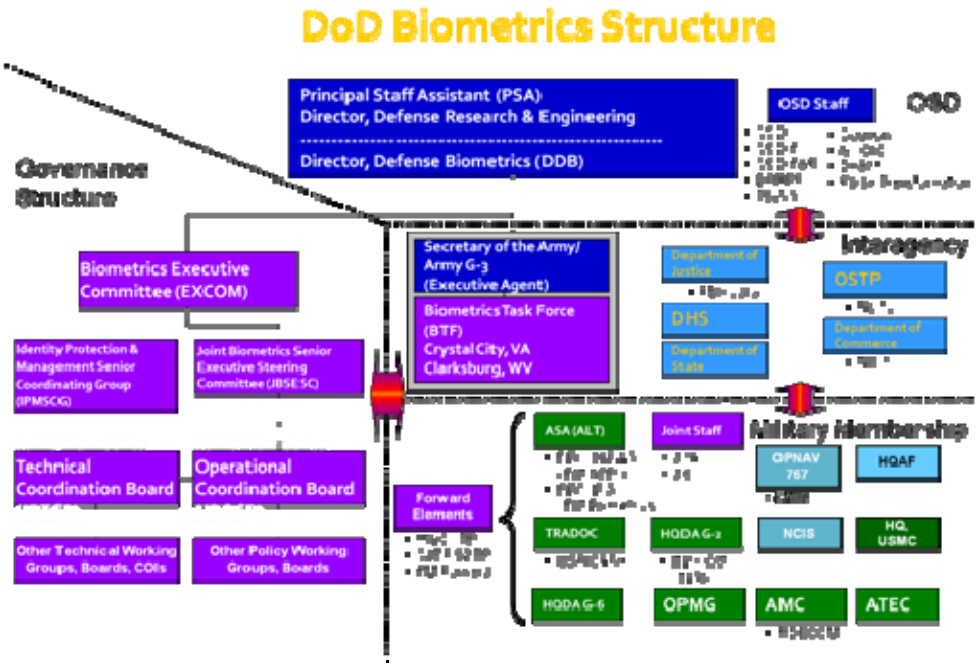


Figure 3. Biometrics Task Force Chain of Command

2. Biometrics Task Force Structure

Internally, the Biometrics Task Force has grown substantially since 2000 to include all of the directors, directorates, divisions displayed in Figure 4 (Lohman). The facilities of the Biometrics Operations Directorate (BOD) that I specifically toured or was exposed to in one form or fashion — Operations, Resource & Support, and Technical

Management Divisions; as well as the twelve branches supporting the Directorate — are located in Clarksburg, WV. The divisions and branches of the Biometrics Integration Directorate (BID) are located in Crystal City, VA. There is a clear and purposeful separation of the operational side of the house from the policy and plans side. One of the strongest reasons is to maximize and build upon the relationship between the FBI Criminal Justice Information Services (CJIS) and BTF operational elements (Zanger). This research will focus mainly on the Biometrics Operations Directorate of the BTF.

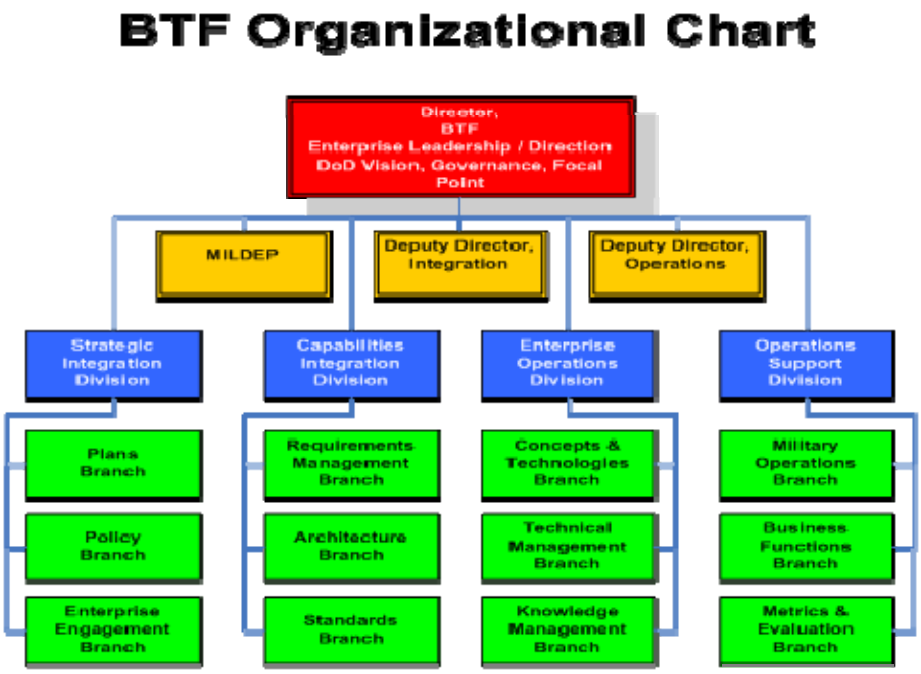


Figure 4. Biometrics Task Force Organizational Chart

3. Biometrics Operations Directorate

The Biometrics Operations Directorate has three main jobs: (1) operate the Automated Biometrics Identification System (ABIS) database containing Red and Gray Forces biometrics data, (2) test and evaluate biometrics equipment, and (3) support field operations of the equipment in use by the Services whether in theater or in the Continental United States (Biometrics Task Force). Within the Biometrics Operations Directorate, there are three divisions with one being the Operations Division. The Operations Division has two missions. The first mission is to provide immediate and

direct support to biometrics cells in Iraq and Afghanistan. The Operations Division accomplishes this by being responsible for coordinating and managing issues and requests for information from the Combatant Commanders (COCOM) on all matters biometrics. Its second role is to drive efforts throughout the Joint Forces to establish comprehensive biometrics training programs. This longer term goal focuses on creating biometrics organizations within all COCOMs, developing a premiere operations center to support worldwide biometrics operations, and institutionalizing biometrics training (Biometrics Task Force).

In order to help emphasize the push that biometrics was moving from theory to operations, the BTF was transferred from the Army's Communications, Information, and Systems Directorate (CIO/G-6) to the Training and Operations Directorate (G-3/5/7) during FY07. In addition, the Army and BTF deployed a Biometrics Torch Party to Iraq in early 2007 to begin standardizing issuance and training of biometrics equipment to units, developing biometrics concepts of operations (CONOPS) and standard operating procedures (SOPs), as well as increasing enrollments and watch list nominations. The success of these Torch Parties in both Iraq and Afghanistan has led to approved Joint Manning Documents that will create permanent 11-man biometrics cells within both theater Headquarters (Biometrics Task Force).

The second and third divisions within the Biometrics Operations Directorate are the Resources & Support Division (R&SD) and the Technical Management Division (TMD). The Resources and Support Division of the Operations Directorate exists simply and plainly to support the BTF. R&SD and its branches implement information technology, maintain overall security of facilities and resources, and manage all BTF resources across the DoD to support the Executive Manager for DoD Biometrics. The Technical Management Division ensures the integrity and availability of the DoD's biometrics data for appropriate users, and performs assessment, integration, interoperability, and testing of biometrics devices (Biometrics Task Force). All new biometrics equipment must be tested and evaluated to ensure compliance with applicable ABIS and data standards. In short, it has to be able to interface with ABIS and not create any vulnerability to the database (Zanger).

4. Joint Forces Initiatives

Although not specifically part of any Biometrics Operations Directorate mission or focus, it is important to understand how the results of the Operations Directorate are implemented around the globe in a theater's daily operations. Through the Joint, Interagency, Multinational Coordination Branch of the BID, the Biometrics Task Force works directly with most of the Army's sister Services in developing, testing, and fielding biometrics technologies. More directly, the coordination between the Biometrics Task Force, U.S. Navy, and United States Marines Corp (USMC) has created substantial gains in biometric capabilities directed toward the Global War on Terrorism. The U.S. Navy (since 2000 when it assigned its first liaison to the BTF) and the USMC (since 2005 when it did the same) have been collaborating with the BTF on multiple IdM and biometric activities. The following is a highlighted list of accomplishments that have occurred up to and through FY07 (Biometrics Task Force):

a. Expanded Maritime Interception Operations (EMIO)

To support the collection and processing of biometric activities during Visit, Board, Search, and Seizure (VBSS) operations, the BTF worked with the Navy to identify and purchase robust biometric equipment; to develop data transmission standards; and, to establish appropriate procedures. The BTF's Automated Biometrics Identification System (ABIS) provides near real-time search and response capabilities.

EMIO Wireless Bridge. Navy and BTF worked to develop a wireless transmission capability compatible with ABIS. 30-plus ships are funded by the Navy for the Wireless Bridge capability.

Tactical Biometrics Collection and Matching System (TBCMS). BTF provided funds to the Navy to develop a small, lightweight, ruggedized system to replace initial bulky biometric systems used for VBSS. TCBMS was delivered in FY 07 after the BTF completed laboratory and ABIS compatibility testing.

b. Identity Dominance System (IDS)

BTF has supported Navy efforts for a holistic multimodal biometrics system of collection and verification that is scalable to different mission profiles. IDS is being designed for interoperability, adherence to technical standards / policies, and network security accreditation. In particular, the BTF has supported the Navy's efforts with document reviews, recommendations, and support through the Joint Staff review process.

c. USMC Biometr ic BAT- HIIDE (Biometrics Automated Toolset — Handheld Intera gency Ide ntity Dete ction Equipment) Collaboration Initiatives

(1) Fielded BAT and HIIDE training elements at Marine Air-Ground Task Force (MAGTF) Integrated Systems Training Centers for each Marine Expeditionary Force (MEF).

(2) Provided BAT and HIIDE equipment to the USMC Corrections Specialist School at Lackland AFB.

(3) Successfully conducted first, complete, biometrics, data refresh while underway during pre-deployment work-ups with the 22nd Marine Expeditionary Unit (MEU).

(4) Deployed 17 biometric field engineers to support Marines at the battalion level assigned to Multinational Forces — West.

d. Latent Print Laboratory

In coordination with Joint Chiefs of Staff, USN, BTF, and Naval Criminal Investigative Service (NCIS), established a Latent Print Laboratory at Camp Fallujah, Iraq to process latent fingerprints from military and terrorist crime scenes.

C. THE DOD BIOMETRICS DATABASE — AUTOMATED BIOMETRICS IDENTIFICATION SYSTEM (ABIS)

1. The Evolution of ABIS

Following the terrorist attacks on September 11, 2001, the DoD evolved its vision for biometrics to include the positive identification of known and suspected terrorists. In addition to expanding the original intent of securing U.S. facilities and networks, the BMO and BFC would now have to generate a biometrics data collection, transmission, and storage system comparable to and compatible with the FBI's Integrated Automated Fingerprint Identification System (IAFIS) (Biometrics Task Force). Three years later the DoD's Automated Biometrics Identification System (ABIS) became operational. ABIS serves as THE central storage for all DoD biometrics data, as well as being able to functionally cross-reference and exchange data with the FBI's IAFIS. ABIS is physically located in the BTF — West facilities in Clarksburg. It is currently manned twenty-four hours a day/ seven days a week by contractors thanks to increases in manning and budgets, as compared to initially being manned on an as needed basis outside normal hours. The day-to-day operation and maintenance of ABIS is being maintained under a Northrop- Grumman contract until the contract comes up for renewal at the end of FY 2009 (Zanger).

2. Basic Daily Operation

So how does ABIS basically work? The quad-chart in Figure 5 below gives a good visual summary of ABIS and its functioning (Quinn). The ABIS operations center at BTF — West is manned 24/ 7 by a Biometrics Examination Services Team (BEST) in support of operations around the globe. They can send and receive data over Unclassified and Classified networks depending on the customer and their capabilities. Within a small room in the BTF — West facilities, there are a large number of widescreen TVs and monitors that display a constant flow of requested fingerprint analysis against the ABIS and/or IAFIS databases. These requests are monitored by specially trained I3 personnel who verify each transaction for compatibility with the ABIS database; make appropriate

changes to requests as necessary to ensure completeness; or, pass along the request to a Latent Print or Ten-Print Examiner (LPE or TPE) for further investigation when there is no match in the database (Zanger). Each request coming in from around the world must be structured as close as possible to the Electronic Biometrics Transmission Specification (EBTS) to be processed by DoD's ABIS or the FBI's IAFIS. Without the correct structure, it is difficult, sometimes impossible, for the ABIS operators to efficiently or effectively conduct a database query.

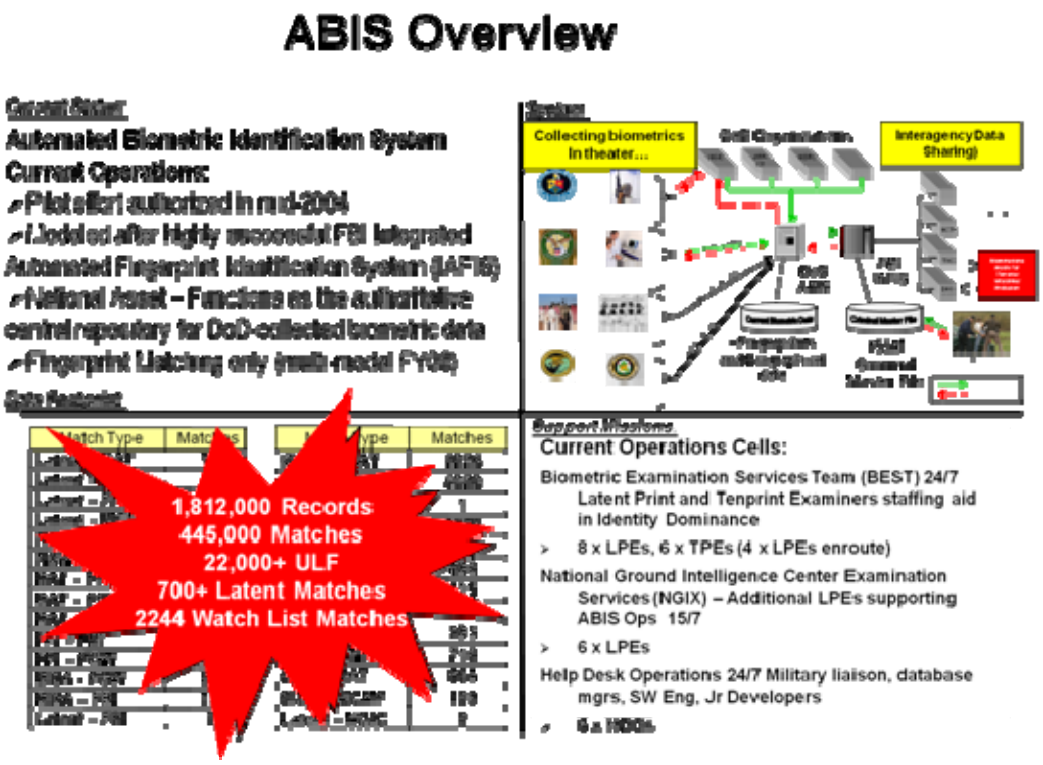


Figure 5. ABIS Quad-Chart Overview

It is important to recognize the continuing need for a "person-in-the-loop" regarding ten print and latent print evaluators any time ABIS or IAFIS does not generate a match. The dedicated TPE's and LPE's support BEST operations 24/7 alongside the ABIS operators. TPE's and LPE's also share the same office space in close proximity to their ABIS operator brethren. This closeness enables greater coordination and efficiency in supporting the boots on the ground. The manual process of evaluating partial, fragmented, or distorted fingerprints will continue to be required until an ABIS or

database querying algorithm is created that can work off the smallest portion of a fingerprint. The algorithms are getting better all the time, but this will probably still not happen anytime soon. Meanwhile, operators are *still* sending to the BTF old fashioned, black ink, individual finger rolled print cards (Zanger).

3. The Identity Dominance Process

Within the DoD's IdM and biometrics lexicon, the formal process from ground pounder to the database and back to the ground pounder is known as the Identity Dominance Process. The Identity Dominance Process is comprised of five steps: (1) Collection, (2) Transmission, (3) Matching, (4) Storing / Sharing, and (5) Analysis. Collection is performed at the pointy end of the spear where multimodal biometrics data, biographical data, and contextual event data about the circumstances surrounding the reason for the collection are gathered and logged. Transmission is self-explanatory and occurs by any means possible or available to the user /customer (e.g., NIPR, SIPR, SAT…). However sent, the data must somehow reach the biometrics repository. Matching occurs either automatically through a database query or manually through human fingerprint examiners (e.g., TPE or LPE). Storing and sharing involves the requirement that every piece of data sent, no matter how small, is permanently collected for potential future use. Secondly, the results of the match query and the updated data are now transmitted back to the User and are made available for interagency sharing. Lastly, Analysis deals with the development of watch lists, possible exploitation by the Intelligence or Information Warfare communities, and Force Protection (Quinn). Figure 6 presents a current example of the Identity Dominance Process.

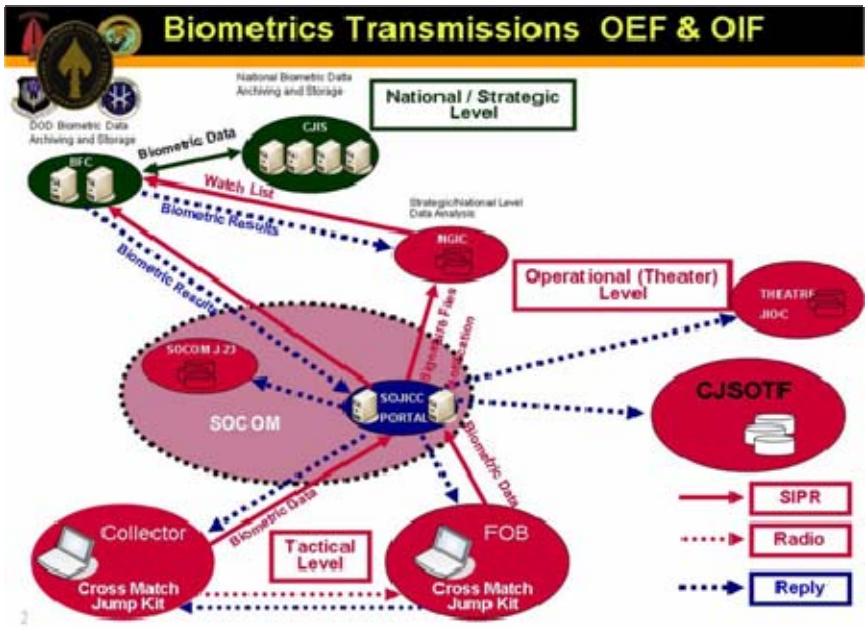


Figure 6. Identity Dominance Process Overview

4. ABIS 2.0: NGA — Next Generation ABIS

In January 2009, a major upgrade to the current ABIS system — NGA or Next Generation ABIS — became operational (Zanger). It provides qualitative improvements over ABIS 1.0 in a multitude of areas. One of the most prominent will be NGA's ability to process multi-modal (fingerprints, iris, face, palm…) biometrics data. Early operational results have shown that NGA can process biometrics in roughly one-third the time of ABIS 1.0. It has also been able to positively match and ID a greater percentage of known or suspected terrorists due to its multi-modal capabilities. To make the new system more manageable, scalable and responsive, NGA was originally designed to be partitioned into four different functional levels: Enterprise, Operational, Regional, and Man-portable. The Enterprise ABIS is the 'Master Database' comprised of all Red and Gray Forces biometrics and relevant data with an initial capacity for over 2 million records. Operational ABIS (e.g., CENTCOM) was expected to be a subset of approximately 500K to 2 million records that will be populated with likely individuals to be encountered in a specific AOR. Regional ABIS (e.g., CJTF-HOA) was to be comprised of roughly 20K to 1 million individuals likely to be encountered. Man-

portable ABIS (e.g., Special Forces Operations) was proposed to be loaded onto ruggedized laptops with databases configured for specific mission needs. Operational and Regional ABIS records were to be located on separate blade servers in the overall Enterprise ABIS server system. Operational, Regional, and Man-portable were all to be fully recoverable and replicated from the Enterprise database as often as required or requested. Each level was also to have Latent/Ten-print Examiner (LPE/TPE) capabilities of one extent or another. Finally, all levels were to be integrated into a Terror Watchlist (Quinn). In the end, however, NGA was able to avoid all the redundancy of data and resources without diminishing capability. Operational connectivity in various AOR's are required to maintain such a specific capacity that NIPR, SIPR, and wireless network connections have the capability to connect directly with NGA. Therefore, Operational, Regional, and Man-portable versions of NGA have become unnecessary. A summary visual of the originally proposed system is provided below in Figure 7.

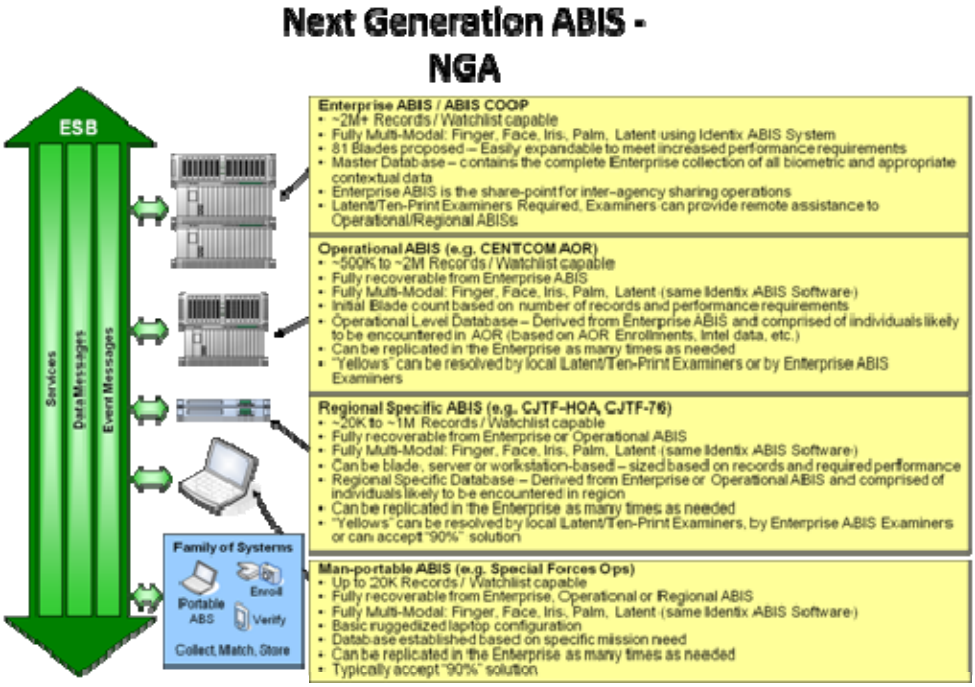


Figure 7. Next Generation ABIS Overview

D. RELATIONSHIPS AND THE FUTURE

1. The BTF and FBI

As mentioned earlier, a major impetus behind the original Biometrics Fusion Center (BFC) was to take advantage of the FBI's technological capabilities and institutional knowledge about biometrics. A lot of the BFC's original biometrics operational concepts and database structure were heavily influenced on known, tested FBI capabilities. Not by coincidence, the Federal Bureau of Investigations also has its CJIS campus located in Clarksburg, WV (Zanger)[5]. To continue to foster interagency teamwork, current long range DoD plans are for the BTF to partner with the FBI to build a joint BTF-W and FBI CJIS facility on CJIS's current property. The DoD has already programmed funding for the joint facility, whereas the FBI is still awaiting funding approval. If the FBI is unable to procure funding, the DoD will fall back to a planned separate facility co-located on the CJIS property. In either case, the intent is to continue to leverage each other's capabilities and maximize the potential from interoperable, interagency biometrics capabilities (Biometrics Task Force).

2. The Near Term

Although the primary focus will always be on supporting the Warfighter, the Biometrics Task Force is collaborating with other services and agencies to move beyond just evaluating technologies that identify Red Forces or Grey Forces. The near-term has seen a shift towards more active design, testing, and implementation of Blue Force business process biometrics (Zanger). Such biometrics business processes include uses for health care records, prescription drugs, financial transactions, Humanitarian Assistance, Refugee Tracking, First Responders, and even re-enlistments. One of the more prominent programs is IDProTECT, or Identification-based Decision Processes to Enable Confident Transactions. IDProTECT is working towards providing a deployable system to enroll, verify, identify, and extract fingerprint and iris biometrics for members

[5] The location of both facilities so near each other had some help from an important individual. Each owes a lot to the Senior Senator from West Virginia — Robert C. Byrd.

who are eligible for enrollment in the Defense Manpower Data Center. The goal is to make IDProTECT a net-centric capable system that can store, search, and match multimodal biometrics that can operate within current privacy acts, laws, and policies (Lohman). Figure 8 below shows the IDProTECT concept in an informative quad chart. Programs like this are intended to help the DoD and her agencies to more accurately identify and track their own people and what business activities they can or cannot undertake. This is the next wave in biometrics for the DoD and the Biometrics Task Force.

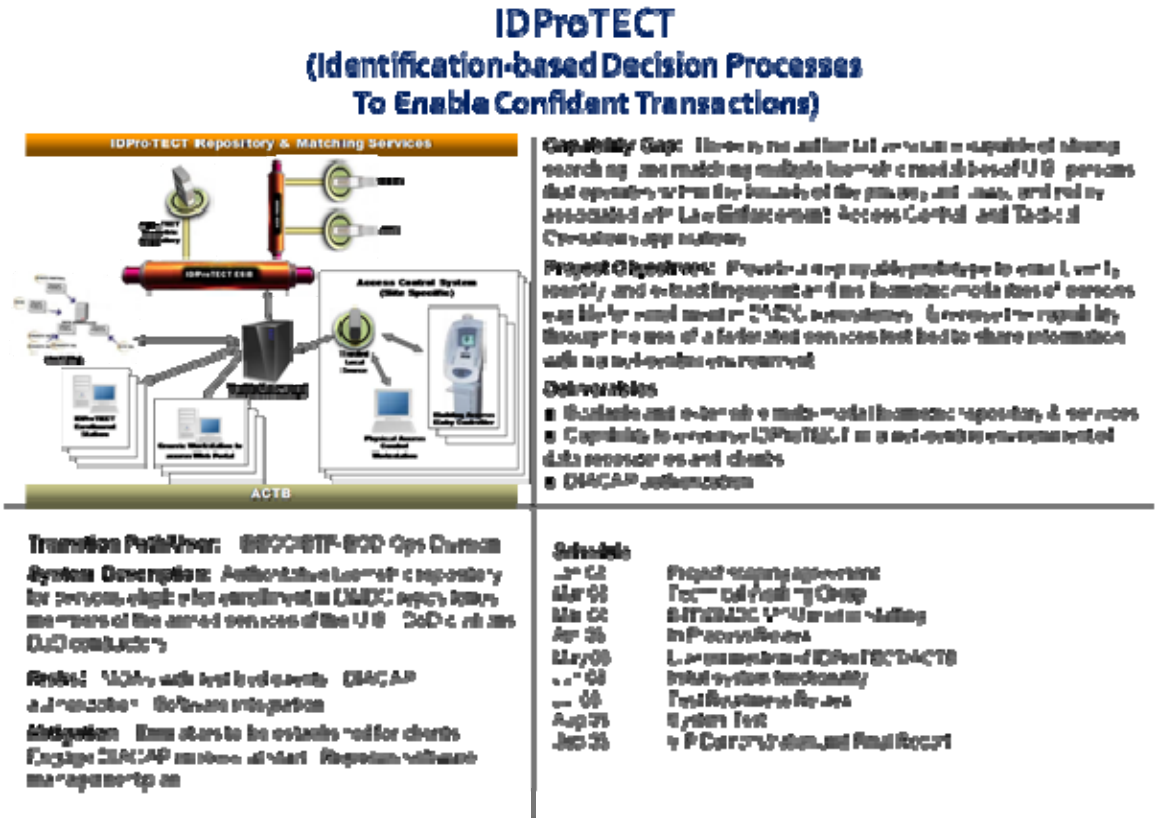


Figure 8. IDProTECT Overview

THIS PAGE INTENTIONALLY LEFT BLANK

IV. BIOMETRIC MODALITIES & FUTURE OPTIONS

A. CURRENT POPULAR BIOMETRIC MODALITIES

1. Basic Biometrics Concepts

Biometrics are simply measurable characteristics of an individual. These characteristics can be subdivided into two categories — anatomical and behavioral. Examples of anatomical biometrics are fingers, iris, face, and hands. Anatomical biometrics systems account for the vast majority of past and present biometric systems. Behavioral biometrics includes models such as signature, gate or walking, and even typing rhythm. Although these might offer the potential to be more discriminating from anatomical biometrics, they are more difficult to measure because of variances across time. If, for example, a biometric system is able to positively ID an individual by his gate, would that same system be able to positively ID the same individual with a broken leg?

Despite biometric systems and technology slowly becoming more typical, biometrics has specific issues that do not help promote faster trust and integration. The biggest of these concerns is the lack of standardization. It most cases individual vendors are creating proprietary equipment that can only be used as per their specifications. Biometrics has not become a truly plug-and-play resource. Within the DoD, this issue is partially being addressed by the BTF. All new operational biometrics systems are technically supposed to be tested through the BTF before being deployed. In most cases this is happening, but there are still outliers such as Special Operations Command who test and field their biometrics independently. Appendix C gives a concise representation of biometrics timeline within the USG for the most significant biometric milestones since 1967 (National Science & Technology Council 8-11). Proprietary systems lead to other issues like a lack of interoperability or scalability. As mandated or self-imposed standards evolve within the biometrics community, large business with the resources to implement biometrics will no longer be the only ones capable of doing so. Standards will

allow businesses of any scale to install and leverage biometrics with whatever technology they currently operate. Lastly, biometric systems and their use have sometimes acquired a connotation with an Orwellian Big Brother keeping track of every strand of DNA or personal detail. A lack of general public knowledge on biometrics combined with a lack of open discussion and detailed product advertising has created an atmosphere of the unknown when it comes to biometrics. Whatever the public does not understand, it will not feel comfortable purchasing, let alone using.

If biometrics is to become as ubiquitous as USB thumb drives, the biometrics community and the federal government need to do more than let technology early adapters drive the momentum. Appendix D highlights some operational milestones of biometrics within the federal government (National Science & Technology Council 23-24). Privacy issues can be countered with information like the fact that biometric data is separate from personal data. Proprietary or otherwise developed biometrics systems take individual biometrics and process them through separate software algorithms. These algorithms have been shown to be fully resistant to reverse-engineering back to the original biometric (National Biometric Security Project 5; sec. 1). Because biometrics connect an individual to a stored digital identity, a business or organization can use this identity to allow or restrict both physical and logical access to resources. Information assurance and IdM specialists can work with network administrators to set access controls appropriate for the individual's role. If incorporated properly, an organization can save resources in both time and money by using biometrics throughout its operations. With the growing access to and falling prices for biometrics, the average user can buy information systems, like a laptop, with biometrics incorporated for a small additional price. As these individual users become more comfortable with biometrics and personally see their value, the word will spread more rapidly. This thesis was produced on a Dell laptop with a fingerprint biometric reader. Being one of the basic users in the population, I have personally benefitted from the ease of use and added security of biometrics. Every laptop I buy in the future will have a biometric reader for security as a result of the confidence I have from their use, whether it comes pre-installed or as an added option.

In the Identity Triad mentioned in Chapter 2, biometrics gives the highest level of assurance by enabling identification through "something you are," over "something you know" and "something you have." Regardless of the improved capability to ID an individual, biometrics is not seen as the end-all to identification. The common belief is that biometrics should be used *in combination* with other technologies to offer true strong authentication (e.g., Use of CAC, strong passwords, and biometrics to be identified and verified by an IdM system). The level of security required for physical and logical access to a specific system or facility will determine the necessary combinations of technologies.

All biometric systems process biometrics in essentially the same manner, just through different technologies. Each system is a pattern recognition system that is used to collect a biometric for enrollment, process the captured biometric using vendor-based algorithms, and then store or attempt to compare for identification or verification to an enrolled digital template of the biometric. This basic process is depicted in Figure 9 (National Biometric Security Project 6; sec. 2). The captured digital biometric is often referred to as the biometric template from which all other potential identifications or verifications will be referenced against. Templates are frequently referenced against a token or password for greater access control depending on the level of security desired. With some technologies, it is necessary to collect multiple images in order to generate a quality template. A biometric systems' ability to generate a quality template for future use, and therefore determine its utility, is dependent on the software's algorithm processing. As has been mentioned previously, the difficulty with incorporating biometric systems into existing information architectures is the proprietary algorithms by which individual companies enroll and verify biometrics require excess resources to adapt.

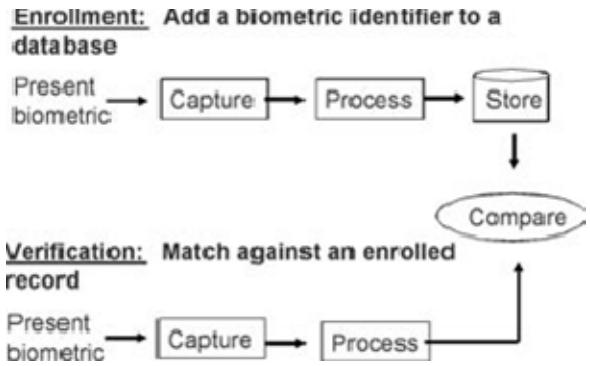


Figure 9. General Biometric System

Because each biometric technology has strengths and weaknesses based on the intended application, it is important to have a complete and clear understanding of the intended usage for the biometric before researching or purchasing the technology. The following is a list of categories that can be used to evaluate the application of a biometric:

1) **Overt or covert systems**—Will the user proactively and knowingly be identified by the system or will it be designed to covertly scan the secured area? Either way, a person must have a biometric template on file for him/her to be recognized.

2) **Voluntary or involuntary systems**—Will system users be required to participate in the system to receive access or benefits, or are there opt-out or work-around options?

3) **Attended or non-attended systems**—Will the system be designed for people to use in a remote location, without assistance? Or will users always have technical assistance and/or attendants available? Involuntary and/or covert systems may always require supervision or attendance to monitor system use. Voluntary and/or overt systems may be "unattended."

4) **Standard or non-standard operating environments**—How much customization will be required for the readers to operate appropriately and

the network to communicate and function properly? Will the system be used outdoors or indoors? Outdoors environments typically fall into "non-standard" operating environments.

5) **Public or private systems**—Is the use of the biometric system for a public program or access to a public facility, or for access to a private company or information? Cooperation with the biometric system can often be directly attributed to whether a system is public or private (i.e., employees).

6) **Physical security and access control**—Are users trying to gain access to a facility or area?

7) **Cyber and computer/network security**—Are users trying to gain access to a computer or protect information on a computer or the Internet?

8) **Identification**—Is the biometric being used for identification purposes for access to benefits, information, border crossing, licensing, etc.? (National Biometric Security Project 10-12; sec. 2).

Biometrics can generate positive identifications in one of two modes — *identification* or *verification*. When operating in an identification mode, a biometrics system is attempting to determine whether or not a given biometric sample matches any of all known biometric templates within a system's database. This is often referred to as a one-to-many (1:N) or open-set identification and is used in applications applicable to law enforcement or terrorist watch lists. The verification process attempts to match a given biometric template against a stored template for a specific user. This is often referred to as a one-to-one (1:1) or closed-set identification. During the enrollment process, the user associates their name, and ID number, or even a token with their biometric template to later verify their identity (National Biometric Security Project 12; sec. 2). Because no system works to one hundred percent perfection, there are two general classes of possible errors that biometrics can create during identification or verification. The first is a *comparison error* where the machine's functioning can generate either a *false match* or *false non-match*. A false match is an incorrect template

match to a given biometric. A false non-match is a false conclusion that a given template is not in the system's database. A second class of error is a *decision error* based on the erroneous assessment from a comparison error (National Biometric Security Project 14; sec. 2). When a system mistakenly matches a given biometric to a database template, the system's application generates a *false accept* and allows access to the system as a result. Further, the probability that this will actually occur with a particular system's application is known as the *false accept rate* — FAR. If the biometric system's application mistakenly concludes that a given biometric template does not reside in the database, the application generates a *false reject* and will deny access. Probability of the application rejecting a valid biometric is termed the *false reject rate* — FRR.

Although not all encompassing by any means, the previous paragraphs offer enough detail to allow a generalized understanding and details by which to compare different biometric technologies. More thorough comparisons of the technologies would require researching the ease of different biometrics to enroll Users, different template storage options, specific components of biometric systems, operational applications for biometrics, and how different biometrics perform in specific IdM architectures. These fall outside the intended scope of this thesis, and can be researched separately.

2. Fingerprint Recognition

Fingerprint recognition is the oldest and most widely used biometric for both business and operational processes. British law enforcement first began to use manual fingerprint identification of criminals in the late nineteenth century. In the 1960s, fingerprint recognition and identification began to move from a manual to an automated process with the introduction of computers. With the assistance of the National Institute for Standards and Technology (NIST), the FBI began to research the automatic classification, searching and matching of fingerprints in the late 1960s (NSTC — Fingerprint 1). Over the next thirty years, the FBI progressed from basic scanners and automated inked fingerprint digitizers to the current fully automated IAFIS system described brifely in Chapter III. Despite initial roll-outs of stand-alone state and international law enforcement fingerprint recognition systems based on individual

standards, fingerprint recognition systems both within the U.S. and internationally have increasingly adopted common standards to allow greater exchange of fingerprint data.

A digital scan or manual roll of a fingerprint will look like a series of alternating dark and white lines. The dark portions of the fingerprint represent *ridges*, and the white space valleys. The location where ridges stop are termed *ridge endings*. Where the ridges split are termed ridge *bifurcations*. Ridge endings and bifurcations are further known as fingerprint *minutae*. In the most general sense, the patterns created by these two distinguishing features or the location of specific minutae help build a model for individual fingerprints that can be used to uniquely ID someone. Fingerprint recognition software is generally designed to either match overall fingerprint patterns or minutae patterns. Figure 10 gives an example of different types of fingerprint images and terminology to describe features (NSTC — Fingerprint 3). Hardware can collect fingerprints individually, four to five fingers at a time, or all ten fingerprints simultaneously. These collections can then either be *slap* or *rolled*. Slapped fingerprints collect an image from the fingernail to the first knuckle. Rolled prints collect images from one side of a fingernail to the other side. The best device to use will varies by the time available to capture images and the intended purpose of the fingerprint system.

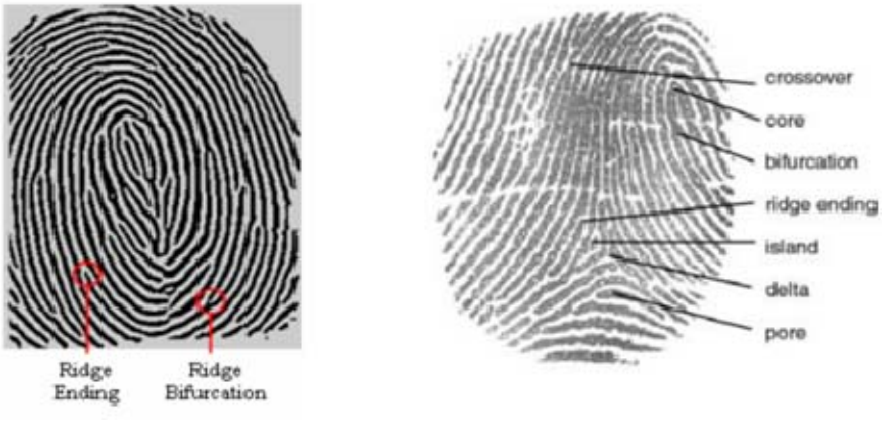


Figure 10. General Fingerprint Characteristics

3. Iris Recognition

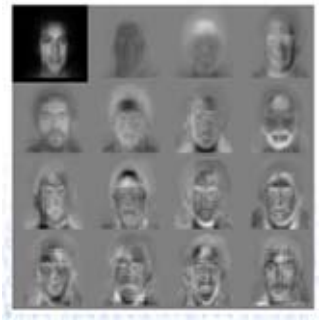
Iris recognition is one of the newer biometric modalities used today in IdM. An automated method for recognizing irises did not receive a patent until 1994 (NSTC — Iris 1). Iris recognition is reasonably straight-forward. The structure or pattern and color of an individual's irises are developed prior to birth and remain stable over a lifetime. Even though an person's irises are genetically the same, their individual irises have separate and distinct patterns. To perform iris recognition, a digital image of the pattern in an iris is collected and quantified using a low or high-resolution camera. Before the image can be taken, however, the iris must be localized to exclude "image noise" from eyelashes, eyelids, pupils, reflections (NSTC — Iris 2). The collected image is then mapped by dividing the iris into *phasors* or segments. Each phasor is mapped for its orientation within the iris along with the iris' individual pattern. The final image generated is referred to as an IrisCode® and becomes the basis for future comparisons. Figure 11 visually represents both the basic structure of an eye and two sample irises.

Figure 11. Iris Diagram and Structure

4. Facial Recognition

Facial recognition is reasonably one of the most innate biometric modalities since most people use the face to recognize one another anyway. Despite the intuitiveness of facial recognition as a concept, the process of facial recognition is far from being standardized with any specific recognition method dominating. The different approaches

to facial recognition are geometric (facial features based), photometric (view based), and algorithm based. Within the algorithm based approach, there are three major types of algorithms — Principal Components Analysis (PCA), Linear Discriminant Analysis (LDA), and Elastic Bunch Graph Matching (EBGM) (NSTC — Face 2). PCA uses a collected image in comparison to a gallery of algorithmic generated images referred to as eigenfaces[6]. Both the collected and gallery images generally require a full frontal image. LDA uses a statistically analytic algorithm to classify an image against within-class (within individual's class of photos) or against samples of images between-class (across all individual image classes) (NSTC — Face 3). EBGM focuses on the non-linear characteristics of real images such as pose, illumination, or expression to generate an elastic grid image with "Gabor jets" that mark distinctive facial nodes (National Biometric Security Project 7; sec. 3). The three algorithms are visualized in Figure 12.

(1)  (2) 

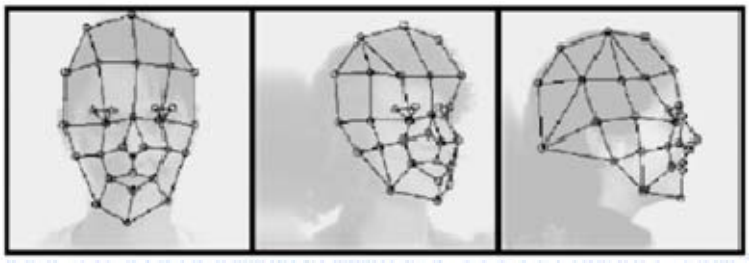
(3) 

Figure 12. (1) PCA, (2) LDA and (3) EBGM Facial Recognition Examples

[6] Eigenfaces is derived from the well known mathematical technique of Principal Component Analysis based on eigen vectors.

B. BEHAVIORAL BIOMETRICS

1. Overview of Behavioral Biometrics

Behavioral biometrics are defined as behavioral traits learned and acquired over time, rather than ones based primarily on biology (National Biometric Security Project 41; sec. 2). The most dominant forms of behavioral biometrics are voice recognition and dynamic signature. Newer potential behavioral biometrics include gait recognition (i.e., the manner in which a person walks) and typing recognition. Using behavioral biometrics can add a fourth dimension — *something you do* — to the ID Trinity as a result of the obvious requirement for the individual to perform an action as part of the verification process. This fourth dimension strengthens the security benefits of one or more of the original three forms of the ID Trinity when used in combination. This should intuitively make sense. If a static biometric statistically offers the highest level of certainty in positive identification, a behavioral biometric which is acquired over years of repetition and also distinctly personal will provide an even greater magnitude of certainty if appropriately processed. The ability to generate an algorithm which quickly and without excessive repetition captures a template, and then make minute adjustments over time, is the hurdle to overcome for successful behavioral biometrics.

2. Voice Recognition

Voice recognition, sometimes also referred to as speaker verification, is a behavioral biometric that uses the voice of an individual to positively make an authentication. Each person's voice is influenced by the physical structure of their vocal tract as well as behavioral characteristics like mouth movement and pronunciation. Voice recognition should not be confused with speech recognition that recognizes spoken words and is not a type of biometric. There are two forms of voice recognition — text-dependent and text-independent (NSTC — Speaker 2). When using the text-dependent method, an individual must present the same specific password or phrase used during enrollment. Text-dependent speaker recognition increases the performance of a

biometric system because the system has a preprogrammed model for comparison. Text-independent systems offer greater flexibility because there does not need to be any specific word of phrase for enrollment or verification. Speech variations in duration, intensity, or pitch are modeled into multiple vector "states" to be used for later verification. The representation of a voice sample plotting voice loudness in the top and voice spectral analysis in the bottom is shown in Figure 13.

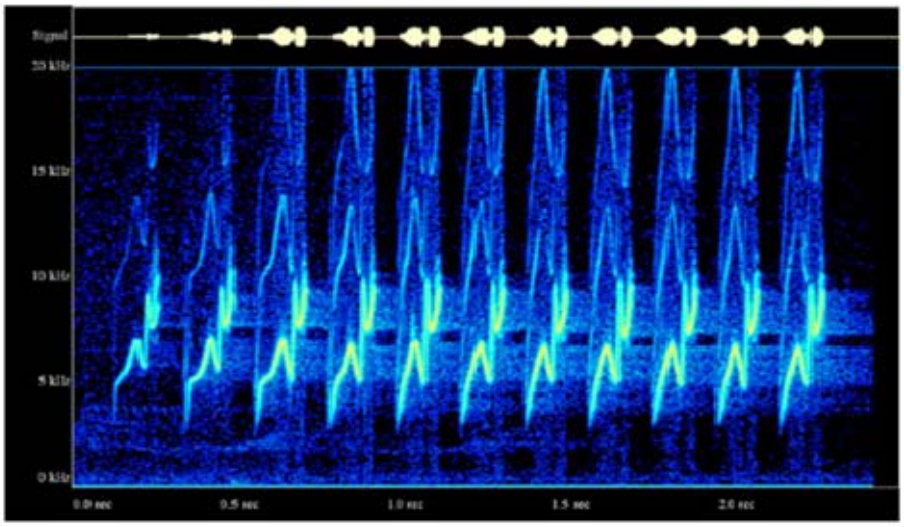


Figure 13. Speaker Recognition Voice Sample

Voice recognition is a popular behavioral biometric because of its low cost and ease of use. A voice recognition system can be layered on top of already existing telephone or cell phone lines which reduce start-up and long-term infrastructure costs. Prevalent uses for voice recognition include physical access control to spaces, phone banking, call center authentication (e.g., home alarm systems), and even house arrest monitoring (National Biometric Security Project 43; sec.3). With the ability to verify an individual remotely, voice recognition can enable automated access to resources or services while simultaneously reducing overhead costs. Drawbacks include susceptibility to transmission noise, inability to control the system used for input if done remotely, and possible spoof attacks using a recorded voice (NSTC — Speaker 4).

3. Dynamic Signature Verification

Dynamic signature verification collects dynamic data such as the speed, pressure, shape, and direction with which an individual writes their signature. After the capture of a few samples to form a template, all the individual is required to do is write their signature for future positive identification. Like many of the other biometrics, dynamic signature verification was not logically possible until computer systems were able to process such algorithms starting in the 1970s. As such, dynamic signature as a tool in IdM is a relatively new option. This biometric should not be confused with the ubiquitous electronic signature capture devices used in the retail or shopping industries. Electronic signature devices simply capture the physical signature for replication and are not a biometric. Figure 14 presents one of many possible options to input a dynamic signature, as well a visual representation of the actual signature and measurements (NSTC — Signature 1).

Because dynamic signatures are nearly impossible to duplicate as compared to a static signature image, it is a very secure method to authenticate an individual. Some dynamic signature algorithms also incorporate learning functions which adjust the individual signature template to account for natural user variability over time.

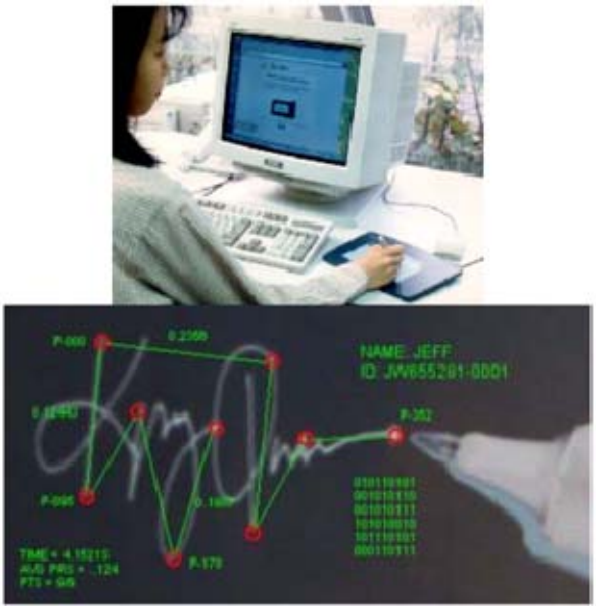


Figure 14. Dynamic Signature Input and Measurements Example

C. USE CASE: BLUE FORCE E-BUISNESS DYANMIC SIGNATURE VERIFICATION

1. The Device: DynaSig Bio-Pen

A dynamic signature biometric like the DynaSig Bio-Pen and accompanying Lock Box software is a flexible security and IdM tool. It is well suited for certain sectors of the business community, like the banking industry or package shipping industry, where identification and verification are mandatory requirements for business processes and auditing. Dynamic signature devices easily incorporate a readily used device — a pen — and accompanying software into current business operations. There is no need for any extensive vendor training, and only a minimal requirement on IT resources. Bank tellers and managers, for example, require an extensive auditing trail to ensure that both the bank and customer are protected from fraud. Signatures in combination with identification like a driver's license have been the standard. The ability to capture in real-time and store indefinitely the verified digital signatures of both customer and bank employee helps nearly eliminate ID fraud and its enormous costs.

The DynaSig Bio-Pen and Lock-Box software offer a simple, user friendly, behavioral biometric toolset for establishing and maintaining secure transactions, IdM, data protection, and a continuous auditing trail. Figure 15 shows a detailed view of the interior components of a Bio-Pen (Kim, Bio-Pen Presentation 6). The Bio-Pen collects motion, pressure, acceleration, timing… in all three axis — X, Y, and Z — through the onboard equipment. Each pen is individually serialized in the hardware to provide a unique ID to the owner and to the firmware when the USB is connected. Every time the Bio-Pen is used, it generates a unique code, equivalent to a time-stamp, to counter potential replay attacks. When an owner writes with the Bio-Pen, the software algorithm creates a unique "signature" that is combined with the two previous pieces of data, encrypted, and sent to the database for comparison (Kim, Bio-Pen White Paper: Security Features). The verified combination of all three pieces of encrypted data provides a high level of security and trust that the person using the pen and the dynamic signature presented are all valid.

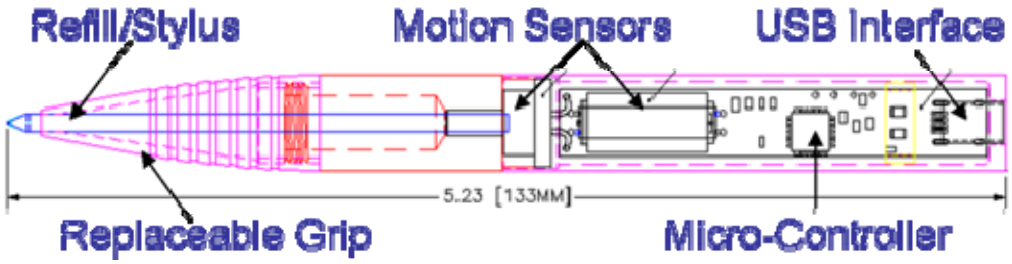


Figure 15. DynaSig Bio-Pen Components

Figure 16 displays some of the Bio-Pen tip and body options available. The Bio-Pen can be configured to work with an ink cartridge as a normal pen, with a stylus designed for PDA's, or even with a stylus designed for Tablet PC's (Kim, Bio-Pen Applications 5). The configuration of the pen is flexible to the business process or requirement, and is easily reconfigurable to move from one to the next.

Figure 16. DynaSig Bio-Pen Tip & Body Options

Along with the digital measures of security explained previously, the combination Bio-Pen and Lock Box software offer some other distinct advantages:

1. Writing a signature is an instinctive, habitual behavioral action.
2. Nearly impossible to impersonate an individual dynamic signature.
3. No passwords to lose or remember.

4. No personal data is created or attached to the system.
5. Personal authentication can be accomplished from anywhere with an Internet connection.
6. Highly scalable to the needs and size of an organization.
7. Software adapts to dynamic signature variation over time through automated updates.
8. Digital and, if desired, physical auditing data ensure non-repudiation.

Like any other dynamic signature biometric, there are a few potential drawbacks depending on the working environment:

1. Owner or User must be able to write a signature.
2. Users with continuously variable signatures will have difficulty enrolling and verifying.
3. Software must be able to adjust for variations in signature over time.
4. Best applications are staff, administration, business, and e-business environments.

2. The Scenario: Military Logistics Tracking and Authorization

Twenty-four hours a day — seven days a week, the four U.S. military Services prepare, transport, and deliver vital military equipment and resources. Like many other global businesses, the four Services need to positively verify that the right materials were loaded onto the right transport, arrived at the right location, and were delivered to the intended customer on time. If something did not go according to the plan, there needs to be a secure real-time system that allows the logistical chain of command to access the most current information and determine a new course of action. The information which will be used for current and future planning can only be trusted if the individual updating the system can be verified for both positive identification and system access privileges, then has their verified identity attached to the data for non-repudiation and auditing.

Without a reliable verification tool as part of an Identity Management Architecture to assure these requirements, all information is suspect until proven otherwise.

This problem has multiple parts that need to be addressed simultaneously in order to at least maintain or preferably improve the data entry, individual verification, and logistic processing timeline. Here are some of the more important questions that need to be addressed: How can the system positively ID each individual? Can there be assurance that the individual identified is not an imposter? How can the system then attach the ID to their data? How can the system ensure the individual entering data is authorized and accredited? Is it possible to do all this in real-time? Is there a method or device which ensures the highest level of security while not mandating added layers of requirements and resources?

In short, yes. Specifically, the DynaSig Bio-Pen dynamic signature device can meet these requirements while easily integrating into whatever logistics process is being performed. From the moment resources are ordered, an audit trail is being produced for current and future use. The person who orders the materials can either do it in person with physical paperwork, or more expeditiously through digital documents. The customer must be verified and offer proof of eligibility by generally signing a document. Whether in a physical or digital signature, the Bio-Pen dynamic signature device can be used to complete the order. From this stage and at every logistic point of processing thereafter, each individual offers their signature as part of the process. Their verified signature will instantaneously and automatically be added to the business process documents, as well as the systems' auditing mechanism. This data will then be available to all access approved individuals. Even if a physical auditing trail is required at one specific location, the Bio-Pen can simultaneously write an ink signature and digital signature fulfilling the requirement.

At any point in the process a higher degree of security such as CAC access to an information system can be added. Individual commands can tailor their specific security requirements while the entire system is assured of the data and the data's owner. Dynamic signatures provide a nearly impossible to duplicate behavioral biometric with an inherently high level of security. If a product like the DynaSig Bio-Pen is

incorporated into the process, the individual using the pen will be known to have been vetted for and given specific access control privileges. A DynaSig Bio-Pen would be ubiquitous in its operation because everyone throughout the chain of command has or is required to use their signature at some point. There is no requirement for any form of training. In summary, a DynaSig Bio-Pen is a low cost, easy to use, behavioral biometric that scales to even the largest enterprise architecture. A dynamic signature verification process layered onto any logistical process instantly provides increased IdM, security, and accountability with little or no system modification.

THIS PAGE INTENTIONALLY LEFT BLANK

V. SUMMARY AND RECOMMENDATIONS

A. SUMMARY

The federal government and all its agencies are working very hard to determine how best to implement a realistic and executable Federal Identity Management Enterprise. Simultaneously, these efforts are not being effectively coordinated despite the unanimous understanding that standardization and coordination are necessary key elements. Regardless of the necessity or agreement, there are always agencies, departments or individuals who do not want to share their information or feel only their ideas are acceptable. These issues are unavoidable and serve only to slow the IdM Enterprise from gaining momentum and being implemented. Despite the real or perceived roadblocks, progress is being made towards universal solutions. Eventual IdM Enterprise systems will spring from the systems being used and developed today. In the DoD, such precursor systems include the Biometric Identification System for Access (BISA) used to identify non-military personnel trying to gain access to coalition facilities, or the Defense Biometrics Identifications System (DBIDS) which verifies personnel trying to gain access to U.S. military facilities and is operated by the Defense Manpower Data Center (DMDC) through military law enforcement. Individual systems like these will be evaluated over time for ease of use, security of data, effectiveness, and scalability. Systems that excel will be expanded. The rest will be discontinued. Other federal departments like the Department of Homeland Security and Department of Justice are experimenting with systems in a likewise fashion. In the future, all of these systems will be integrated in either a logical or physical fashion to support a holistic Federal IdM Enterprise.

This thesis attempted to take a snapshot in time of the current state of affairs in federal IdM and biometrics, while specifically focusing on the Department of Defense. The information contained in this thesis is by no means all encompassing. It should be considered nothing more than a significant primer on the subjects at best. Necessary and substantial topics that will also need to be addressed include: (1) legal issues concerning

the collection, storage, and use of U.S. citizen personal data; (2) social implications to gaining widespread use and trust of identity management tools like biometrics; and, (3) development of standards that enable physically separate systems to exchange data logically in order to meet operational or business needs. No holistic solution is possible without addressing and presenting long-term solutions that stay within the boundaries of the U.S. Constitution, meet process requirements, and guarantee the security and integrity of the data.

B. RECOMMENDATIONS

The field of Identity Management does not have the recognition or precedence behind it commensurate with its current value. Every day people are walking across U.S. borders or landing at U.S. airports trying to gain access to the nation. No one needs to be reminded the country is at war, and the requirement for maintaining the security of American citizens never stops. Billions of tax-payer funded dollars are stolen annually through identity theft because minimally paid or under skilled workers are entrusted with safeguarding personal data on technology they do not understand. Even worse, these federal or state employees sometimes just sell the data or credentials to make a quick buck without regard to their fellow citizens and to the damage to their country. What do agencies do when breaches happen? In some cases, the incidence and its details are kept in close hold. It is hoped that in most cases, the breach, those victimized, and a solution are presented to help minimize the damage. In either case, potential and actual victims are at the mercy of the agency for information because there is no reciprocity in regards to personal data access. Only the agencies and its employees have access to an individual's collected personal data. Outcomes such as these arising from unsecured personal data on USG systems which lack full transparency are no longer acceptable to the American public.

First, resources and focus must be put into education. Educating the personnel who will operate current and future IdM architectures within an overarching Federal IdM Enterprise must be a priority. Academic institutions like West Virginia University and the Naval Postgraduate School have seen this requirement and have implemented courses

of instruction towards that end. West Virginia University has targeted undergraduate and graduate courses in biometrics, identity management, and computer security. The Naval Postgraduate School recently established a federal certification in Identity Management tailored purposely for military and civil service professionals in the biometrics and IdM fields. If federal and state governments make it known that these particular fields are of great concern, public and private educational institutions will invest the resources to create applicable course and degrees.

Secondly, all agencies and departments of the federal government must acknowledge that a new field of IdM professionals is vitally required. Within the DoD, the Services need to definitively delineate IdM and biometrics positions or billets from their information technology specialists. For instance, the U.S. Navy's information technology specialists come from the Information Professional (IP) Community. IP's can be detailed to a range of billets with specialties that include information assurance, knowledge management, or communications. There is, however, no recognition for the need to designate or create billets that focus on identity management or biometrics. The Navy and her sister Services need to acknowledge this major oversight, and then work the manning documents to correct. This process and mentality needs to permeate the USG as a whole.

The public is only minimally aware of the impact and influence that IdM and biometrics is going to play in their future daily lives. As thoughtful and logical discussions begin to take place outside the Beltway of Washington, DC, Americans will be exposed to the benefits and detractors of a Federal IdM Enterprise. National, state, and local leaders themselves need to grasp the basic concepts so that they can lead these necessary discussions. The train bringing nationalized IdM and biometrics in some form or fashion has already left the station. Now is the time for the American public to decide what kind of Federal IdM Enterprise they will accept, and their government to implement it.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A — NSTC STRUCTURE

NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

COMMITTEE ON ENVIRONMENT & NATURAL RESOURCES		
AIR QUALITY RESEARCH (SC)	GLOBAL CHANGE RESEARCH/ CLIMATE CHANGE SCIENCE (SC)	US GROUP ON EARTH OBSERVATIONS (SC)
DISASTER REDUCTION (SC)	OCEAN SCIENCE & TECHNOLOGY (SC)	WATER AVAILABILITY & QUALITY (SC)
ECOLOGICAL SYSTEMS (SC)	TOXICS AND RISK (SC)	

COMMITTEE ON HOMELAND & NATIONAL SECURITY		
DECONTAMINATION STANDARDS & TECHNOLOGY (SC)	HUMAN FACTORS (SC)	STANDARDS (SC)
DOMESTIC IMPROVISED EXPLOSIVE DEVICES (SC)	INFRASTRUCTURE (SC)	
FOREIGN ANIMAL DISEASE THREAT (SC)	NUCLEAR DEFENSE RESEARCH & DEVELOPMENT (SC)	

COMMITTEE ON SCIENCE		
AQUACULTURE (SC)	HUMAN SUBJECTS RESEARCH (SC)	RESEARCH BUSINESS MODELS (SC)
BIOTECHNOLOGY (SC)	LARGE SCALE SCIENCE (SC)	SCIENCE TO SUPPORT FOOD & AGRICULTURAL RESEARCH (TF)
DIGITAL DATA (IWG)	PHYSICS OF THE UNIVERSE (IWG)	SCIENTIFIC COLLECTIONS (IWG)
DOMESTIC ANIMAL GENOMICS (IWG)	PLANT GENOMES (IWG)	SOCIAL, BEHAVIORAL, ECONOMIC SCIENCES (SC)
EDUCATION & WORKFORCE DEVELOPMENT (SC)	PRION SCIENCE (IWG)	

COMMITTEE ON TECHNOLOGY		
AERONAUTICS (SC)	HYDROGEN & FUEL CELLS (IWG)	NANOSCALE SCIENCE, ENGINEERING & TECH. (SC)
BIOMETRICS & IDENTITY MANAGEMENT (SC)	INNOVATION & COMPETITIVENESS (SC)	NETWORKING & INFORMATION TECHNOLOGY (SC)
BUILDINGS TECHNOLOGY RESEARCH & DEV. (SC)	MANUFACTURING RESEARCH & DEVELOPMENT (IWG)	

October 2008

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B — NSTC BIOMETRICS GLOSSARY & ACRONYMS

Version 1.0

Biometrics Glossary (BG)

Feb 1, 2008

A

American National Standards Institute (ANSI)

A private, non-profit organization that administers and coordinates the U.S. voluntary standardization and conformity assessment system. The mission of ANSI is to enhance both the global competitiveness of U.S. business and the U.S. quality of life by promoting and facilitating voluntary consensus standards and conformity assessment systems, and safeguarding their integrity.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Analyze

Converts data to actionable information and recommendations as applicable to increase situational awareness and better understand possible courses of action.

Derived from Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Arch

A fingerprint pattern in which the friction ridges enter from one side, make a rise in the center, and exit on the opposite side. The pattern will contain no true delta point.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Associated Information

Non-biometric information about a person. For example, a person's name, personal habits, age, current and past addresses, current and past employers, telephone number, email address, place of birth, family names, nationality, education level, group affiliations, and history, including such characteristics as nationality, educational achievements, employer, security clearances, financial and credit history.

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Attempt

The submission of a single set of biometric samples to a biometric system for identification or verification. Some biometric systems permit more than one attempt to identify or verify an individual.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Authoritative Source

The primary DoD-approved repository of biometric information on a biometric subject. The authoritative source provides a strategic capability for access to standardized, comprehensive, and current biometric files within the DoD and for the sharing of biometric files with Joint, Interagency, and designated Multinational partners. The DoD may designate authoritative sources for various populations consistent with applicable law, policy and directives.

Derived from Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Auto-correlation	A proprietary finger scanning technique. Two identical finger images are overlaid in the auto-correlation process, so that light and dark areas, known as Moiré fringes, are created. *International Association for Biometrics (iAfB) and International Computer Security Association (ICSA), 1999 Glossary of Biometric Terms* http://www.afb.org.uk/docs/glossary.htm
Automated Biometric Identification System (ABIS)	Department of Defense (DoD) system implemented to improve the U.S. government's ability to track and identify national security threats. *National Science & Technology Council (NSTC), 14 September 06* http://www.biometrics.gov/Documents/glossary.pdf
Automated Fingerprint Identification System (AFIS)	A highly specialized biometric system that compares a submitted fingerprint record (usually of multiple fingers) to a database of records, to determine the identity of an individual. AFIS is predominantly used for law enforcement, but is also being used for civil applications (e.g. background checks for soccer coaches, etc). *National Science & Technology Council (NSTC), 14 September 06* http://www.biometrics.gov/Documents/glossary.pdf
Automated Identification Management System (AIMS)	A system that acts as a central web-based informational portal between U.S. Central Command (USCENTCOM), National Ground Intelligence Center (NGIC), and the Biometrics Fusion Center (BFC) that is designed to fuse intelligence analysis and value added comments from field users of matched biometric and biographic data. *USCENTCOM Biometric Identification System for Access (BISA) CONOPS*

B

Behavioral Biometric Characteristic

A biometric characteristic that is learned and acquired over time rather than one based primarily on biology. All biometric characteristics depend somewhat upon both behavioral and biological characteristic. Examples of biometric modalities for which behavioral characteristics may dominate include signature recognition and keystroke dynamics.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Bifurcation

The point in a fingerprint where a friction ridge divides or splits to form two ridges.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Biographic Data

Data that describes physical and non-physical attributes of a biometric subject from whom biometric sample data has been collected. For example, full name, age, height, weight, address, employers, telephone number, email address, birthplace, nationality, education level, group affiliations, also data such as employer, security clearances financial and credit history.

Derived from USCENTCOM Biometric Identification System for Access (BISA) CONOPS

Biological Biometric Characteristic

A biometric characteristic based primarily on an anatomical or physiological characteristic, rather than a learned behavior. All biometric characteristics depend somewhat upon both behavioral and biological characteristics. Examples of biometric modalities for which biological characteristics may dominate include fingerprint and hand geometry.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Biometrically Enabled Intelligence

Intelligence information associated with biometrics data e.g. pattern analysis of a biometric subject's encounters with biometrics systems, judgments about a biometric subject disposition or intent based on biometric matches with forensic data, etc.

Derived from DoD D 8521.AAE DoD BIOMETRICS PROGRAM

Biometrically Enabled Physical Access

The process of granting access to installations and facilities through the use of biometrics.

Derived from Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Biometrically Enabled Watchlist (BEWL)

Any list of person of interests (POI), with individuals identified by biometric sample instead of by name, and the desired/recommended disposition instructions for each individual. However, there first must be an acceptable degree of certainty that there is some indication of past behavior attributable to the individual that belongs to the biometric sample in order to estimate the level of threat posed by that individual. Even upon encounter or capture, we may never know an individuals' true identity, but that is immaterial as long as the linkage between the biometric sample and past threat behavior is established. No practicable standard currently exists for BEWLs, but the minimum content of a BEWL record is (1) a biometric identity (biometric sample linked to a POI), (2) a category of interest or threat commonly referred to as a tier, (3) the recommended action(s) to taken upon next encounter, and (4) notification instructions. The classification of the information within the BEWL can be up to TS/SCI/ORCON. In most instances the information will be releasable or at the UNCLASSIFIED//FOUO level to facilitate sharing.

The DoD Biometrically-Enabled Watchlist (BEWL) A Federated Approach, May 3, 2007

Biometric Application Decision

A conclusion based on the application decision policy after consideration of one or more comparison decisions, comparison scores and possibly other non-biometric data.

JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007

Biometric Automated Toolset (BAT)

A multimodal biometric system that collects and compares fingerprints, iris images and facial photos. It is used to enroll, identify and track persons of interest; build digital dossiers on the individuals that include interrogation reports, biographic information, relationships, etc. BAT has an internal biometric signature searching and matching capability.

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Biometric Capture Device

A device that collects a signal from a biometric characteristic and converts it to a captured biometric sample.

JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007

Biometric Capture Process

A process of collecting or attempting to collect signals from a biometric characteristic and converting them to a captured biometric sample.

JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007

Biometric Characteristic

A biological and behavioral characteristic of a biometric subject that can be detected and from which distinguishing, repeatable biometric features can be extracted for the purpose of automated recognition of biometric subjects.

	Derived from JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007
Biometric Claim	A claim that a biometric subject is or is not the source of a specified or unspecified biometric reference. *JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007*
Biometric Database	A collection of one or more computer files. For biometric systems, these files could consist of biometric sensor readings, templates, match results, related biometric subject information, etc. *Derived from National Science & Technology Council (NSTC), 14 September 06* *http://www.biometrics.gov/Documents/glossary.pdf*
Biometric Data Block	A block of data with a defined format that contains one or more biometric samples or biometric templates. *JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007*
Biometric Feature	Numbers or labels extracted from biometric samples and used for comparison. *JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007*
Biometric Feature Extraction Process	A process applied to a biometric sample with the intent of isolating and outputting repeatable and distinctive numbers or labels which can be compared to those extracted from the other biometric samples. *JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007*
Biometric File	The standardized individual data set resulting from a collection action (biometric sample and contextual data). *Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006*
Biometric Identification Application	A system which contains an open-set or closed-set identification application. *JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007*

Biometric Identification System for Access (BISA)

A biometric and contextual data collection and credential card production system. It is capable of multi-modal biometric collection (fingerprint, iris, and facial recognition). The system collects biometric and biographical information from visitors to U.S., Coalition, and allied installations worldwide. It produces biometric enabled identification cards compatible with the Common Access Card (CAC) readers. The identification cards (which are counterfeit deterrent, tamper proof and encrypted), use fingerprint images to conduct one-to-one identity verification. BISA collects, transmits, stores, retrieves, manipulates, and displays biometric and contextual data in accordance with national/international standards and industry best practices.

Initial Capabilities Document (ICD) for Biometrics in Support of Personnel Identity (BSPI) (Draft), 30 Jun 07

Biometric Intelligence Resource (BIR)

A system that has been established to provide members of the DoDIIS Intelligence Community and theater war fighters with access to a reliable, centralized, and permanent repository of potential terrorist biometric information and associated intelligence information. The BIR system ingests biometric signatures and contextual data collected from Department of Defense biometric processing systems and makes this information available to members of the worldwide Intelligence Community through a web-based interface for the purpose of positive identification of individuals and tracking related intelligence.

Derived from Biometric Intelligence Resource (BIR) Implementation: 2006-2007 BIR Version 2 System Design Document (SDD) 20 June 2007

Biometric Property

The descriptive attributes of the biometric subject estimated or derived from the biometric sample by automated means.
EXAMPLE Fingerprints can be classified by the biometric properties of ridge-flow, i.e. arch whorl and loop types. In the case of facial recognition, this could be estimates of age or gender.

JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007

Biometric Reference

One or more stored biometric samples, biometric templates or biometric models attributed to a biometric subject and used for comparison.
EXAMPLE Face image on a passport; fingerprint minutia(e) template on a National ID card; Gaussian Mixture Model for speaker recognition, in a database.

JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007

Biometrics

A general term used alternatively to describe a characteristic or a process.
As a characteristic: A measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition.
As a process: Automated methods of recognizing a biometric subject based on measurable biological (anatomical and physiological) and behavioral characteristics.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Biometric Sample	One of two components of a biometric file (biometric samples and contextual data). Data that represents a biometric characteristic of a biometric subject as captured by a biometric system. *Derived from Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006*
Biometric Sample Collector	An individual trained in biometrics that is familiar with employment of biometrics in support of his or her organization, performing the biometric sample(s) collection. *Biometrics Task Force & Biometrics Data Team*
Biometrics Application Programming Interface (BioAPI)	Defines the application programming interface and service provider interface for a standard biometric technology interface. The BioAPI enables biometric devices to be easily installed, integrated or swapped within the overall system architecture. *National Science & Technology Council (NSTC), 14 September 06* http://www.biometrics.gov/Documents/glossary.pdf
Biometrics Enterprise	All systems, interfaces and personnel that are utilized to establish identities of people through the use of biometric modalities. *Biometrics Task Force Strategy Division*
Biometrics Program	A comprehensive process incorporating the principles and practices of biometrics into an organization. *DoD D 8521.AAE DoD BIOMETRICS PROGRAM*
Biometric Subject	An individual for which biometric samples were collected and enrolled into a biometric database for the purpose of identification and/or verification. *Biometrics Task Force & Biometrics Data Team*
Biometric System	Multiple individual components (such as sensor, matching algorithm, and result display) that combine to make a fully operational system. A biometric system is an automated system capable of: 1. Capturing a biometric sample from a biometric subject. 2. Extracting and processing the biometric data from that sample. 3. Storing the extracted information in a database. 4. Comparing the biometric data with data contained in one or more references. 5. Deciding how well they match and indicating whether or not an identification or verification of identity has been achieved. A biometric system may be a component of a larger system. *Derived from National Science & Technology Council (NSTC), 14 September 06* http://www.biometrics.gov/Documents/glossary.pdf

Biometric Template	Set of stored biometric features comparable directly to biometric features of a recognition biometric sample. *JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007*
Blue Force	A population group of trusted individuals including, but not limited to, DoD personnel and family members, U.S. persons, trusted allies, and coalition members. *DoD D 8521.AAE DoD BIOMETRICS PROGRAM*

C

Challenge Response

A method used to confirm the presence of an individual by eliciting direct responses from the individual. Responses can be either voluntary or involuntary. In a voluntary response, the individual will consciously react to something that the system presents. In an involuntary response, the individual body automatically responds to a stimulus. A challenge response can be used to protect the system against attacks.

Derived from National Science & Technology Council (NSTC), 14 September 06
http://www.biometrics.gov/Documents/glossary.pdf

Closed-set Identification

A biometric task where an unidentified biometric subject is known to be in the database and the system attempts to determine his/her identity. Performance is measured by the frequency with which the biometric subject appears in the system's top rank (or top 5, 10, etc.).

Derived from National Science & Technology Council (NSTC), 14 September 06
http://www.biometrics.gov/Documents/glossary.pdf

Collect

Capture biometric and related contextual data from a biometric subject, with or without his knowledge. Create and transmit a standardized, high-quality biometric file consisting of a biometric sample and contextual data to a data source for matching.

Derived from Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Common Access Card (CAC)

The standards identification card for active duty personnel (to include the selected reserve), DoD civilian personnel, and eligible contractor personnel. It is the principal card used to enable physical access to buildings and controlled spaces and can be used to gain access to the department's computer networks and systems. The card, which accommodates an integrated circuit chip, also contains other relevant media such as magnetic strips and bar codes.

DoD Deputy Secretary of Defense Memorandum, Smart Card Adoption and Implementation, 10 November 1999

Common Biometric Exchange File Format (CBEFF)

A standard that provides the ability for a system to identify, and interface with multiple biometric systems, and to exchange data between system components.

National Science & Technology Council (NSTC), 14 September 06
http://www.biometrics.gov/Documents/glossary.pdf

Common Biometric Exchange Formats Framework (CBEFF) specification

Describes a set of data elements necessary to support biometric technologies in a common way. These data can be placed in a single file used to exchange biometric information between different system components or between systems. The result promotes interoperability of biometric-based application programs and systems developed by different vendors by allowing biometric data interchange.

National Institute of Standards and Technology Interagency Report (NISTIR) 6529-2001, Common Biometric Exchange File Format, 3 January 2001

Comparison	Process of comparing a biometric reference with a previously stored reference or references in order to make an identification or verification decision. *National Science & Technology Council (NSTC), 14 September 06* *http://www.biometrics.gov/Documents/glossary.pdf*
Comparison Decision	Determination of whether the recognition biometric sample(s) and biometric reference(s) have the same biometric source, based on a comparison score(s), a decision policy(ies), including a threshold, and possibly other inputs. *JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007*
Contextual Data	Elements of biographical and situational information (who, what, when, where, how, why, etc.) that are associated with a collection event and permanently recorded as an integral component of the biometric file. *Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006*
Core Point	The 'center(s)' of a fingerprint. In a whorl pattern, the core point is found in the middle of the spiral/circles. In a loop pattern, the core point is found in the top region of the innermost loop. More technically, a core point is defined as the topmost point on the innermost upwardly curving friction ridgeline. A fingerprint may have multiple cores or no cores. *National Science & Technology Council (NSTC), 14 September 06* *http://www.biometrics.gov/Documents/glossary.pdf*
Cumulative Match Characteristic (CMC)	A method of showing measured accuracy performance of a biometric system operating in the closed-set identification task. Templates are compared and ranked based on their similarity. The CMC shows how often the biometric subject template appears in the ranks (1, 5, 10, 100, etc.), based on the match rate. A CMC compares the rank (1, 5, 10, 100, etc.) versus identification rate. *National Science & Technology Council (NSTC), 14 September 06* *http://www.biometrics.gov/Documents/glossary.pdf*

D

Decide/Act

The response by the operational or business process owner (either automated or human-in-the-loop) to the results of the match and/or analysis described in the DoD Biometric Process, as well as associated information relevant to the situation.

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Defense Biometrics Identification System (DBIDS)

A DoD owned and operated system developed by Defense Manpower Data Center (DMDC) as a force protection program to manage installation access control for military installations. It is a networked client/server database system designed to easily verify the access authorization of personnel and fingerprint biometric identification. The DBIDS software application is used to enter personnel and vehicle data into a database, capture biometric information, and retrieve that data and biometric information for verification and validation at a later time.

Defense Biometric Identification System User Manual, May 24, 2006

Degrees of Freedom

A statistical measure of how unique biometric data is. Technically, it is the number of statistically independent features (parameters) contained in biometric data.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Delta Point

The part of a fingerprint pattern that looks similar to the Greek letter delta. Technically, it is the point on a friction ridge at or nearest to the point of divergence of two type lines, and located at or directly in front of the point of divergence.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Detainee Reporting System (DRS)

A System designed to support the processing of prisoner of wars (POWs) and detainees by issuing Identification Serial Numbers (ISNs), collecting identifying information, recording medical histories, maintaining property records, issuing transfer, release, death, and other orders providing dispositions to detainees, maintain a tribunal history, and track changes to detainee records and other general information relevant to the detainee.

Derived from Detainee Reporting System courtesy of National Detainee Reporting Center, August 06

Detection and Identification Rate

The rate at which biometric subjects, who are in a database, are properly identified in an open-set identification (watchlist) application.

Derived from National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Detection Error Trade-off (DET) Curve	A graphical plot of measured error rates. DET curves typically plot matching error rates (false non-match rate vs. false match rate) or decision error rates (false reject rate vs. false accept rate). *National Science & Technology Council (NSTC), 14 September 06* *http://www.biometrics.gov/Documents/glossary.pdf*
Difference Score	A value returned by a biometric algorithm that indicates the degree of difference between a biometric sample and a reference. *National Science & Technology Council (NSTC), 14 September 06* *http://www.biometrics.gov/Documents/glossary.pdf*
Duplicate Enrollment Check	The comparison of a recognition biometric sample/biometric feature/biometric model to some or all of the biometric references in the enrollment database to determine if any similar biometric reference exists. *JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007*

E

Electronic Biometric Transmission Specification (EBTS)	Describes customizations of the Federal Bureau of Investigation (FBI) Electronic Fingerprint Transmission Specification (EFTS) transactions that are necessary to utilize the Department of Defense (DoD) Automated Biometric Identification System (ABIS). Any DoD entity that wishes to interface with the DoD ABIS must conform to the DoD EBTS. *Department of Defense* *Electronic Biometric Transmission Specification* *23 August 2005 Version 1.1 DIN: DOD_BMO_TS_EBTS_Aug05_01.01*
Electronic Fingerprint Transmission Specification (EFTS)	A document that specifies requirements to which agencies must adhere to communicate electronically with the Federal Bureau of Investigation (FBI) Integrated Automated Fingerprint Identification System (IAFIS). This specification facilitates information sharing and eliminates the delays associated with fingerprint cards. *National Science & Technology Council (NSTC), 14 September 06* *http://www.biometrics.gov/Documents/glossary.pdf*
Enroll	Create and store, for a biometric subject, an enrollment data record that includes biometric reference(s) and typically, non-biometric data. *Derived from JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007*
Enrollment	The process of collecting a biometric sample from a biometric subject, converting it into a biometric reference, and storing it in the biometric system's database for later comparison. *Derived from National Science & Technology Council (NSTC), 14 September 06* *http://www.biometrics.gov/Documents/glossary.pdf*
Expanded Maritime Interdiction Operation (EMIO)	A key maritime component needed to support the global war on terrorism by deterring, delaying, and disrupting the movement of terrorists and terrorist-related materials and personnel at sea. U.S. Navy ships operating in the Central Command's (CENTCOM) Area of Responsibility (AOR) have the capability to collect and forward biometric data from potential terrorists for searching against databases. *Derived from Biometrics Task Force And Navy Team for Success January 2007*

F

Face Recognition

A biometric modality that uses an image of the visible physical structure of a biometric subject's face for recognition purposes.

Derived from National Science & Technology Council (NSTC), 14 September 06
http://www.biometrics.gov/Documents/glossary.pdf

Failure to Acquire (FTA)

Failure of a biometric system to capture and/or extract usable information from a biometric sample.

National Science & Technology Council (NSTC), 14 September 06
http://www.biometrics.gov/Documents/glossary.pdf

Failure to Acquire Rate

The frequency of a failure to acquire.

National Information Assurance Partnership, US Government Biometric Verification Mode Protection Profile for Medium Robustness Environments v1.0, 15 November 2003, Sponsored by the DoD Biometrics Management Office (BMO) and the National Security Agency (NSA)

Failure to Enroll (FTE)

Failure of a biometric system to form a proper enrollment reference for a biometric subject. Common failures include biometric subjects who are not properly trained to provide their biometrics, the sensor not capturing information correctly, or captured sensor data of insufficient quality to develop a template.

Derived from National Science & Technology Council (NSTC), 14 September 06
http://www.biometrics.gov/Documents/glossary.pdf

Failure to Enroll Rate

The probability that a biometric system will have a failure-to-enroll.

National Information Assurance Partnership, US Government Biometric Verification Mode Protection Profile for Medium Robustness Environments v1.0, 15 November 2003, Sponsored by the DoD Biometrics Management Office (BMO) and the National Security Agency (NSA)

False Acceptance

When a biometric system incorrectly identifies a biometric subject or incorrectly authenticates an imposter against a claimed identity.

Derived from National Information Assurance Partnership, US Government Biometric Verification Mode Protection Profile for Medium Robustness Environments v1.0, 15 November 2003, Sponsored by the DoD Biometrics Management Office (BMO) and the National Security Agency (NSA)

False Acceptance Rate (FAR)

A statistic used to measure biometric performance when operating in the verification task. The percentage of times a system produces a false acceptance, which occurs when a biometric subject is incorrectly matched to another biometric subject's existing biometric. Example: Frank claims to be John and the system verifies the claim.

Derived from National Science & Technology Council (NSTC), 14 September 06

	http://www.biometrics.gov/Documents/glossary.pdf
False Alarm Rate	A statistic used to measure biometric performance when operating in the open-set identification (sometimes referred to as watchlist) task. This is the percentage of times an alarm is incorrectly sounded on a biometric subject who is not in the biometric system's database (the system alarms on Frank when Frank isn't in the database), or an alarm is sounded but the wrong biometric subject is identified (the system alarms on John when John is in the database, but the system thinks John is Steve). *Derived from National Science & Technology Council (NSTC), 14 September 06* http://www.biometrics.gov/Documents/glossary.pdf
False Match	The comparison decision of 'match' for a recognition biometric sample and a biometric reference that are not from the same source. *JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007*
False Match Rate (FMR)	A statistic used to measure biometric performance. Similar to the False Acceptance Rate (FAR). *Derived from National Science & Technology Council (NSTC), 14 September 06* http://www.biometrics.gov/Documents/glossary.pdf
False Non-Match	A comparison decision of 'no-match' for a recognition biometric sample and a biometric reference that are from the same source. *JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007*
False Non-Match Rate (FNMR)	A statistic used to measure biometric performance. Similar to the False Reject Rate (FRR), except the FRR includes the Failure To Acquire error rate and the False Non-Match Rate does not. *National Science & Technology Council (NSTC), 14 September 06* http://www.biometrics.gov/Documents/glossary.pdf
False Rejection	The failure of a biometric system to identify a biometric subject or to verify the legitimate claimed identity of a biometric subject. *Derived from National Information Assurance Partnership, US Government Biometric Verification Mode Protection Profile for Medium Robustness Environments v1.0, 15 November 2003, Sponsored by the DoD Biometrics Management Office (BMO) and the National Security Agency (NSA)*
False Rejection Rate (FRR)	A statistic used to measure biometric performance when operating in the verification task. The percentage of times the system produces a false rejection. A false rejection occurs when a biometric subject is not matched to his/her own existing biometric template. Example: John claims to be John, but the system incorrectly denies the claim.

	Derived from National Science & Technology Council (NSTC), 14 September 06 *http://www.biometrics.gov/Documents/glossary.pdf*
Features	Distinctive mathematical characteristic(s) derived from a biometric sample; used to generate a reference. *National Science & Technology Council (NSTC), 14 September 06* *http://www.biometrics.gov/Documents/glossary.pdf*
Fingerprint	The image left by the minute ridges and valleys found on the hand of every person. In the fingers and thumbs, these ridges form patterns of loops, whorls and arches. *Federal Bureau of Investigation (FBI) website, Taking Legible Fingerprints* *http://www.fbi.gov/hq/cjisd/takingfps.html*
Fingerprint Recognition	A biometric modality that uses the physical structure of an biometric subject's fingerprint for recognition purposes. Important features used in most fingerprint recognition systems are minutia(e) points that include bifurcations and ridge endings. *Derived from National Science & Technology Council (NSTC), 14 September 06* *http://www.biometrics.gov/Documents/glossary.pdf*
Fingerprint Scanning	Acquisition and recognition of a biometric subject's fingerprint characteristics for identification purposes. This process allows the recognition of a biometric subject through quantifiable physiological characteristics that detail the unique identity of an individual. *Derived from The Intel Corporation website, Biometric User Authentication: Fingerprint Sensor Product Guidelines . Version 1.03, September 2003* *http://www.intel.com/design/mobile/platform/downloads/FingerprintSensorProductGuidelines.pdf*
Fingerprint Vendor Technology Evaluation (2003) (FpVTE)	An independently administered technology evaluation of commercial fingerprint matching algorithms. *National Science & Technology Council (NSTC), 14 September 06* *http://www.biometrics.gov/Documents/glossary.pdf*
Force Protection (FP)	Preventive measures taken to mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information by using biometrics to positively link identity information to a given physical individual. Force protection does not include actions to defeat the enemy or protect against accidents, weather, or disease. Also called FP. *Derived from Joint Publication 3-0, Joint Operations,17 September 2006* *http://www.dtic.mil/doctrine/jel/new_pubs/jp3_0.pdf*

Foreign Humanitarian Assistance (FHA)

Programs conducted to relieve or reduce the results of natural or manmade disasters or other endemic conditions such as human pain, disease, hunger, or privation that might present a serious threat to life or that can result in great damage to or loss of property. Foreign humanitarian assistance (FHA) provided by US forces is limited in scope and duration. The foreign assistance provided is designed to supplement or complement the efforts of the host nation civil authorities or agencies that may have the primary responsibility for providing FHA. FHA operations are those conducted outside the United States, its territories, and possessions. Also called FHA. Biometrics can be used as an enabler for personal identification for humanitarian assistance distribution.

Derived from Joint Publication 3-0, Joint Operations, 17 September 2006

http://www.dtic.mil/doctrine/jel/new_pubs/jp3_0.pdf

Forensic

Relates to the use of science or technology in the investigation and establishment of facts or evidence. Collected biometric samples could then be linked to non-biometric forensic evidence.

Derived from Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Friction Ridge

The ridges present on the skin of the fingers and toes, and on the palms and soles of the feet, which make contact with an incident surface under normal touch. On the fingers, the distinctive patterns formed by the friction ridges that make up the fingerprints.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Friendly

Trusted individuals, DoD personnel and family members, US Persons, trusted Allies, Coalition, etc.

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Full Enrollment

Enrollment of biometric data on a subject that includes 14 fingerprint images (4 slaps, 10 rolls), 5 face photos, 2 irises, and required text fields. The sample must be EBTS compliant. Typically used for detainees, locally hire screenings, and other applications.

Initial Capabilities Document (ICD) for Biometrics in Support of Personnel Identity (BSPI) (Draft), 30 Jun 07

G

Gait

A biometric subject's manner of walking. This behavioral characteristic is in the research and development stage of automation.

Derived from National Science & Technology Council (NSTC), 14 September 06
http://www.biometrics.gov/Documents/glossary.pdf

Gallery

The biometric system's database, or set of known biometric subjects, for a specific implementation or evaluation experiment.

Derived from National Science & Technology Council (NSTC), 14 September 06
http://www.biometrics.gov/Documents/glossary.pdf

Gray Force

A general term used to describe civilian personnel. However, the term may also be applied to defined individuals for whom no identity has been positively established. It may include those individuals that have not been positively identified as being either hostile (Red) or friendly (Blue). In general use, it has become a term similar to "Boggy", which is used by aviation personnel to indicate that they have acquired contact (visual or radar) with another aircraft but have not identified it as being friendly or hostile ("Bandit"). A population group of unknown individuals including, but not limited to, nonaligned persons, host country and third-country nationals, and non-U.S. citizens.

Initial Capabilities Document (ICD) for Biometrics in Support of Personnel Identity (BSPI) (Draft), 30 Jun 07

H

Hamming Distance (HD)

The number of non-corresponding digits in a string of binary digits; used to measure dissimilarity. Hamming distances are used in many Daugman iris recognition algorithms.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Hand Geometry Recognition

A biometric modality that uses the physical structure of a biometric subject's hand for recognition purposes.

Derived from National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Hand Scan

Print from the outer side of the palm.

Initial Capabilities Document (ICD) for Biometrics in Support of Personnel Identity (BSPI) (Draft), 30 Jun 07

I

Identification

The one-to-many (1:N) process of comparing a submitted biometric sample against all of the biometric reference templates on file to determine whether it matches any of the templates and, if so, the known identity of the biometric subject whose template was matched.

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Identification Rate

The rate at which a biometric subject in a database is correctly identified.

Derived from National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Identifier

A unique data string used as a key in the biometric system to name a biometric subject's identity and its associated attributes. An example of an identifier would be a passport number.

Derived from National Information Assurance Partnership, US Government Biometric Verification Mode Protection Profile for Medium Robustness Environments v1.0, 15 November 2003, Sponsored by the DoD Biometrics Management Office (BMO) and the National Security Agency (NSA)

Identity

The set of attribute values (i.e. characteristics) by which a biometric subject is recognizable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish that biometric subject from any other biometric subject and to distinguish the identity from any other identity.

Derived from Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Identity Assurance

Operations that protect and defend identity information and management by ensuring their availability, integrity, authentication, confidentiality, intended use (privacy), and non-repudiation.

DoD Biometrics Strategy Working Group

Identity Claim

A statement that a biometric subject is or is not the source of a reference in a database. Claims can be positive (I am in the database), negative (I am not in the database), or specific (I am end user 123 in the database).

Derived from NSTC Sub committee on Biometrics IAW INCITS/M1 and ISO/IEC JIYC 2 SC37standards bodies, Aug 2006.

Identity Dominance

The operational capability to achieve an advantage over an adversary by denying him the ability to mask his identity, or counter our biometric technologies and processes. This is accomplished through the use of enabling technologies and processes to establish the identity of a biometric subject and to establish a knowledge base for that identity.

Derived from Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Identity Governance

The combination of policies and actions taken to ensure enterprise-wide consistency, privacy protection and appropriate interoperability between individual identity management systems.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Identity Management

A business function that authenticates an individual to validate identity, DoD affiliation, and authorization of the credential holder. The centralized data repository delivers credentialing information and status for business functions within DoD for use as proof of identity and DoD affiliation is delivered by Identity Management.

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Identity Protection

The process of safeguarding and ensuring the identities of individuals, devices, applications, and services are not compromised.

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Identity Protection and Management Senior Coordinating Group (IPMSCG)

A DoD-level group that provides the enterprise coordinating framework for identity protection and management elements and activities for individuals, devices, applications, and services and oversee the integration of DoD-wide policy, capabilities and strategy for managing physical and virtual identities.

DoD D 852I.AAE DoD BIOMETRICS PROGRAM

Identity Superiority

The management, protection and dominance of identity information for friendly, neutral or unknown, and adversary subject through the application of military operations and business functions.

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Integrated Automated Fingerprint Identification System (IAFIS)

The FBI's large-scale ten fingerprint (open-set) identification system that is used for criminal history background checks and identification of latent prints discovered at crime scenes. This system provides automated and latent search capabilities, electronic image storage, and electronic exchange of fingerprints and responses.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Intermediate Biometric Sample Processing	Any manipulation of a biometric sample that does not produce biometric features. Example: Intermediate biometric samples may have been enhanced for biometric feature extraction. *JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007*
International Committee for Information Technology Standards (INCITS)	Organization that promotes the effective use of information and communication technology through standardization in a way that balances the interests of all stakeholders and increases the global competitiveness of the member organizations. *National Science & Technology Council (NSTC), 14 September 06* *http://www.biometrics.gov/Documents/glossary.pdf*
Interoperability	The conditions achieved among communications-electronic (CE) equipment systems or items of CE equipment when information or services can be exchanged directly and satisfactorily between them and their users. *Joint Publication 6-0, Joint Communication Systems, 20 March 2006* *http://www.dtic.mil/doctrine/jel/new_pubs/jp6_0.pdf*
Iris Code©	A biometric feature format used in the Daugman iris recognition system. *National Science & Technology Council (NSTC), 14 September 06* *http://www.biometrics.gov/Documents/glossary.pdf*
Iris Recognition	A biometric modality that uses an image of the physical structure of a biometric subject's iris for recognition purposes. The iris muscle is the colored portion of the eye surrounding the pupil. *Derived from National Science & Technology Council (NSTC), 14 September 06* *http://www.biometrics.gov/Documents/glossary.pdf*

K

Keystroke Dynamics A biometric modality that uses the cadence of a biometric subject's typing pattern for recognition.

Derived from National Science & Technology Council (NSTC), 14 September 06
http://www.biometrics.gov/Documents/glossary.pdf

L

Latent Fingerprint

A fingerprint "image" left on a surface that was touched by a biometric subject. The transferred impression is left by the surface contact with the friction ridges, usually caused by the oily residues produced by the sweat glands in the finger.

Derived from National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Latent Sample

A biometric residue that is dormant, inactive, or non-evident but can be captured, measured and stored. It may be difficult to see, but can be made visible to scrutiny. A residue left on a medium that came in contact with a biometric subject.

Derived from Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Live Capture

Typically refers to a fingerprint capture device that electronically captures fingerprint images using a sensor (rather than scanning ink-based fingerprint images on a card or lifting a latent fingerprint from a surface).

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Liveness Detection

A technique used to ensure that the biometric sample submitted is from a biometric subject. A liveness detection method can help protect the system against some types of spoofing attacks.

Derived from National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Live Scan

Occurs when taking a fingerprint or palm print directly from a biometric subject's hand.

Derived from ANSI/NIST-ITL 1-2000, Data Format for the Interchange of Fingerprint, Facial, & Scar mark & Tattoo Information

http://www.itl.nist.gov/ANSIASD/sp500-245-a16.pdf

Locally Employed Personnel (LEP)

A person employed by the Coalition and US military, not US citizens.

USCENTCOM Biometric Identification System for Access (BISA) CONOPS

Local Trusted Source

A sub-set of the Authoritative Source and is established to accomplish a specific function within an operational mission or business process. Reasons for establishing a local trusted source might include: insufficient network connectivity to provide immediate access to the authoritative source, an operational need for closed-loop access, permission application.

Derived from Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Local Un-Trusted Source	A local repository of biometric files that that have not been enrolled with an authoritative or local trusted source. In many cases, local un-trusted sources are established for missions of short duration or to satisfy political, policy, or legal restrictions related to the sharing of biometric information. *Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006*
Logical Access	Process of granting access to information system resources to authorized users, programs, processes, or other systems. The controls and protection mechanisms that limit users' access to information and restrict their forms of access to only what is appropriate. *Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006*
Loop	A fingerprint pattern in which the friction ridges enter from either side, curve sharply and pass out near the same side they entered. This pattern will contain one core and one delta. *National Science & Technology Council (NSTC), 14 September 06* *http://www.biometrics.gov/Documents/glossary.pdf*

M

Match

The process of accurately identifying or verifying the identity of a biometric subject by comparing a standardized biometric file to an existing source of standardized biometric data, and scoring the level of confidence of the match. Matching consists of either a one-to-one (verification) or one-to-many (identification) search.

Derived from Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Mimic

The presentation of a live biometric measure in an attempt to fraudulently impersonate someone other than the submitter.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Minutia(e) Point

The point where a friction ridge begins, terminates, or splits into two or more ridges. Minutia(e) are friction ridge characteristics that are used to individualize a fingerprint image.

ANSI/NIST-ITL 1-2000, Data Format for the Interchange of Fingerprint, Facial, & Scar mark & Tattoo Information

http://www.itl.nist.gov/ANSIASD/sp500-245-a16.pdf

Modality

A type or class of biometric system. For example: face recognition, fingerprint recognition, iris recognition, etc.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Model

A representation used to characterize a biometric subject. Behavioral-based biometric systems, because of the inherently dynamic characteristics, use models rather than static templates.

Derived from National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Multimodal Biometric System

A biometric system in which two or more of the modality components (biometric characteristic, sensor type or feature extraction algorithm) occurs in multiple.

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

N

National Institute of Standards and Technology (NIST)

A non-regulatory federal agency within the U.S. Department of Commerce that develops and promotes measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. NIST's measurement and standards work promotes the well-being of the nation and helps improve, among many others things, the nation's homeland security.

National Institute of Standards and Technology
http://www.nist.gov/public_affairs/factsheet/homeland.htm

National Security Telecommunications and Information Systems Security Committee (NSTISSP #11)

National security community policy governing the acquisition of information assurance (IA) and IA-enabled information technology products.

The National Information Assurance Partnership, Common Criteria Evaluation Validated Scheme, Information Assurance Dictorate FAQ V2.1, 6 January 2002
http://www.niap-ccevs.org/cc-scheme/nstissp_11.pdf

Neutral or Unknown

Nonaligned individuals; host-country and third-country national non-US citizens.

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Non-DoD Partners

Interagency and Multinational partners

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Non-match

A decision that the recognition biometric sample(s) and the biometric reference are not from the same source.

JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007

O

One-to-Many

A phrase used in the biometrics community to describe a system that compares one reference to many enrolled references to make a decision. The phrase typically refers to the identification or watchlist tasks.

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

One-to-One

A phrase used in the biometrics community to describe a system that compares one reference to one enrolled reference to make a decision. The phrase typically refers to the verification task (though not all verification tasks are truly one-to-one). The identification task can be accomplished by a series of one-to-one comparisons.

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Open-set Identification

Biometric task that more closely follows operational biometric system conditions to 1) determine if a biometric subject is in a database and 2) find the record of the biometric subject in the database. This is sometimes referred to as the "watchlist" task to differentiate it from the more commonly referenced closed-set identification.

Derived from National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Operational Evaluation

One of the three types of performance evaluations. The primary goal of an operational evaluation is to determine the workflow impact seen by the addition of a biometric system.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

P

Palm Print Recognition

A biometric modality that uses the physical structure of a biometric subject's palm print for recognition purposes.

Derived from National Science & Technology Council (NSTC), 14 September 06
http://www.biometrics.gov/Documents/glossary.pdf

Performance

A catch-all phrase for describing a measurement of the characteristics, such as accuracy or speed, of a biometric algorithm or system.

National Science & Technology Council (NSTC), 14 September 06
http://www.biometrics.gov/Documents/glossary.pdf

Personal Identification Number (PIN)

A number used in conjunction with an access control system as a secondary credential by the user to ensure the holder of the access control card is the authorized user.

Naval Facilities Engineering Service Center , Antiterrorism Team website, Glossary of Terms

Person Data Exchange Standard (PDES)

A specification of the U.S. government intelligence community that specifies XML tagging of person data, including biometric data.

U.S. Government Person Data Exchange Standard (PDES)

Person of Interest

An individual for whom information needs or discovery objectives exist.

The DoD Biometrically-Enabled Watchlist (BEWL) A Federated Approach, May 3, 2007

Platen

The surface on which a finger is placed during optical finger image capture.

International Association for Biometrics (iAfB) and International Computer Security Association (ICSA), 1999 Glossary of Biometric Terms
http://www.afb.org.uk/docs/glossary.htm

Probe

The biometric sample that is submitted to the biometric system to compare against one or more references in the gallery.

National Science & Technology Council (NSTC), 14 September 06
http://www.biometrics.gov/Documents/glossary.pdf

R

Receiver Operating Characteristics (ROC)

A method of showing measured accuracy performance of a biometric system. A verification ROC compares false acceptance rate vs. verification rate. An open-set identification (watchlist) ROC compares false alarm rates vs. detection and identification rate.

National Science & Technology Council (NSTC), 14 September 06
http://www.biometrics.gov/Documents/glossary.pdf

Recognition

A generic term used in the description of biometric systems (e.g. face recognition or iris recognition) relating to their fundamental function. The term 'recognition' does not inherently imply the verification, closed-set identification or open-set identification (watchlist).

National Science & Technology Council (NSTC), 14 September 06
http://www.biometrics.gov/Documents/glossary.pdf

Red Force

A collective term for enemy or opposing forces. It can include regular military, naval, and air forces as well as irregular combatant forces, terrorists, guerillas, and any other enemy combatant. A population group of individuals including, but not limited too, known enemy combatants, known or suspected terrorists, detainees, criminals, hostile foreign intelligence officers, and persons of interest.

DoD D 852I.AAE DoD BIOMETRICS PROGRAM

Re-enrollment

The process of establishing a new biometrics reference for a biometric subject already enrolled in the database.

JTC001-SC37-N-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007

Reference (Function)

The process of querying various repositories of associated information on individuals (Intelligence, Medical, Human Resources, Financial, Security, Education, Law Enforcement, etc) for analysis purposes.

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Response Time

The time used by a biometric system to return a decision on identification or verification of a biometric sample.

International Association for Biometrics (iAfB) and International Computer Security Association (ICSA), 1999 Glossary of Biometric Terms
http://www.afb.org.uk/docs/glossary.htm

Ridge Ending

A minutiae point at the ending of a friction ridge.

National Science & Technology Council (NSTC), 14 September 06
http://www.biometrics.gov/Documents/glossary.pdf

Rolled Fingerprints

An image that includes fingerprint data from nail to nail, obtained by "rolling" the finger across a sensor.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

S

Scenario Evaluation

One of the three types of performance evaluations. The primary goal of a scenario evaluation is to measure performance of a biometric system operating in a specific application.

National Science & Technology Council (NSTC), 14 September 06
http://www.biometrics.gov/Documents/glossary.pdf

Segmentation

The process of parsing the biometric signal of interest from the entire acquired data system. For example, finding individual finger images from a slap impression.

National Science & Technology Council (NSTC), 14 September 06
http://www.biometrics.gov/Documents/glossary.pdf

Sensor

Hardware found on a biometric device that converts biometric input into a digital signal and conveys this information to the processing device.

National Science & Technology Council (NSTC), 14 September 06
http://www.biometrics.gov/Documents/glossary.pdf

Share

Exchange standardized biometric files and match results among approved Army, DoD, Interagency, and Multinational partners in accordance with applicable law and policy.

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Signature Dynamics

A behavioral biometric modality that analyzes dynamic characteristics of a biometric subject's signature, such as shape of signature, speed of signing, pen pressure when signing, and pen-in-air movements, for recognition.

Derived from National Science & Technology Council (NSTC), 14 September 06
http://www.biometrics.gov/Documents/glossary.pdf

Similarity Score

A value returned by a biometric algorithm that indicates the degree of similarity or correlation between a biometric sample and a reference.

National Science & Technology Council (NSTC), 14 September 06
http://www.biometrics.gov/Documents/glossary.pdf

Slap Fingerprint

Fingerprints taken by simultaneously pressing the four fingers of one hand onto a scanner or a fingerprint card. Slaps are known as four finger simultaneous plain impressions.

National Science & Technology Council (NSTC), 14 September 06
http://www.biometrics.gov/Documents/glossary.pdf

Source

An approved database and infrastructure that stores biometrics files.

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Speaker Recognition	A biometric modality that uses a biometric subject's speech, a feature influenced by both the physical structure of a biometric subject's vocal tract and the behavioral characteristics of the biometric subject, for recognition purposes. Sometimes referred to as 'voice recognition.' 'Speaker Recognition' is not the same as 'Speech recognition' which recognizes the words being said and is not a biometric technology. *Derived from National Science & Technology Council (NSTC), 14 September 06* *http://www.biometrics.gov/Documents/glossary.pdf*
Speech Recognition	A technology that enables a machine to recognize spoken words. Speech recognition is not a biometric technology. *National Science & Technology Council (NSTC), 14 September 06* *http://www.biometrics.gov/Documents/glossary.pdf*
Spoofing	The ability to fool a biometric sensor into recognizing an illegitimate biometric subject as a legitimate biometric subject (Verification) or into missing an identification of someone that is in the database. *Derived from National Science & Technology Council (NSTC), 14 September 06* *http://www.biometrics.gov/Documents/glossary.pdf*
Store	The process of enrolling, maintaining, and updating biometric files to make available standardized, current biometric information on biometric subjects when and where required. Biometric files are either enrolled or updated before they are stored. *Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006*
Submission	The process whereby a subject provides a biometric sample to a biometric system. *National Science & Technology Council (NSTC), 14 September 06* *http://www.biometrics.gov/Documents/glossary.pdf*

T

Tactical Enrollment

Enrollment of biometric data on a subject that includes at least 2 fingerprints (indexes), 2 iris prints, and required text fields. The sample must be EBTS compliant. Typically used when subject is not being detained, but a record of the encounter is required at an ICED site, raid, humanitarian assistance, etc. It is an identification leading to an enrollment of a subject utilizing biometric data that includes at least 1 fingerprint or 1 iris and capture identification number. Used when subject is being detained and full enrollment will be conducted at the detention facility or at a base access point, when a subject is applying for a job on a base and is escorted to the LEP screening site for full enrollment.

Initial Capabilities Document (ICD) for Biometrics in Support of Personnel Identity (BSPI) (Draft), 30 Jun 07

Template

A digital representation of a biometric subject's distinct characteristics, representing information extracted from a biometric sample. Templates are used during biometric authentication as the basis for comparison.

Derived from National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Tethered Biometric System

Use of biometric sensors between deployed personnel within a robust command and control architecture.

Biometrics Fusion Center

Threshold

A user setting for biometric systems operating in the verification or open-set identification (watchlist) tasks. The acceptance or rejection of biometric data is dependent on the match score falling above or below the threshold. The threshold is adjustable so that the biometric system can be more or less strict, depending on the requirements of any given biometric application.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Throughput Rate

The number of biometric transactions that a biometric system processes within a stated time interval.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

True Acceptance Rate

A statistic used to measure biometric performance when operating in the verification task. The percentage of times a system (correctly) verifies a true claim of identity. For example, Frank claims to be Frank and the system verifies the claim.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

True Rejection Rate

A statistic used to measure biometric performance when operating in the verification task. The percentage of times a system (correctly) rejects a false claim of identity. For example, Frank claims to be John and the system rejects the claim.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

U

Untethered Biometric System

Collection, analysis and use of biometric sensors between deployed personnel outside of a robust command and control architecture.

Biometrics Fusion Center

U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT)

A continuum of security measures that begins overseas, at the Department of State's visa issuing posts, and continues through arrival and departure from the United States of America. Using biometrics, such as digital, inkless fingerscans and digital photographs, the identity of visitors requiring a visa is now matched at each step to ensure that the person crossing the U.S. border is the same person who received the visa. For visa-waiver travelers, the capture of biometrics first occurs at the port of entry to the U.S. By checking the biometrics of a traveler against its databases, US-VISIT verifies whether the traveler has previously been determined inadmissible, is a known security risk (including having outstanding wants and warrants), or has previously overstayed the terms of a visa. These entry and exit procedures address the U.S. critical need for tighter security and ongoing commitment to facilitate travel for the millions of legitimate visitors welcomed each year to conduct business, learn, see family, or tour the country.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

V

Valley

The area of a fingerprint surrounding a friction ridge that does not make contact with an incident surface under normal touch; the area of the finger between two friction ridges.

ANSI INCITS 378-2004
Information technology - Finger Minutiae Format for Data Interchange

Verification

The one-to-one process of matching a biometric subject's biometric sample against his stored biometric file. Also known as Authentication.

Derived from Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Verification Rate

A statistic used to measure biometric performance when operating in the verification task. The rate at which legitimate biometric subjects are correctly verified.

Derived from National Science & Technology Council (NSTC), 14 September 06
http://www.biometrics.gov/Documents/glossary.pdf

Vulnerability

The potential for the function of a biometric system to be compromised by intent (fraudulent activity), design flaw (including usage error), accident, hardware failure, or external environmental condition.

National Science & Technology Council (NSTC), 14 September 06
http://www.biometrics.gov/Documents/glossary.pdf

W

Watchlist

A term sometimes referred to as open-set identification that describes one of the three tasks that biometric systems perform. Answers the questions: Is this person in the database? If so, who are they? The biometric system determines if the individual's biometric template matches a biometric template of someone on the watchlist. The individual does not make an identity claim, and in some cases does not personally interact with the system whatsoever.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Wavelet Scalar Quantization (WSQ) Grayscale Fingerprint Image Compression Specification (IAFIS-IC-0010 [V3])

Provides the definitions, requirements, and guidelines for specifying the FBI's WSQ compression algorithm. The document specifies the class of encoders required, decoder process, and coded representations for compressed image data.

Criminal Justice Information Services (CJIS) Electronic Fingerprint Transmission Specification IAFIS-doc-01078-7.1

http://www.fbi.gov/hq/cjisd/iafis/efts71/efts71.pdf

Whorl

A fingerprint pattern in which the ridges are circular or nearly circular. The pattern will contain 2 or more deltas.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

# #

10 Print Match or Identification	An absolute positive identification of a biometric subject by corresponding each of his or her 10 fingerprints to those in a system of record. Usually performed by an AFIS system and verified by a human fingerprint examiner. *Derived from Biometrics Task Force* *http://www.biometrics.dod.mil/ReferenceTutorials/BiometricsGlossary/tabid/87/Default.aspx*

Version 1.0

Biometrics Glossary (BG)

Feb 1, 2008

Acronyms

ABIS	Automated Biometric Identification System
AFIS	Automated Fingerprint Identification System
AIMS	Automated Identification Management System
ANSI	American National Standards Institute
AOR	Area of Responsibility
ASCII	American Standard Code for Information Interchange
BAT	Biometric Automated Toolset
BC	Biometric Consortium
BDT	Biometric Data Team
BFC	Biometric Fusion Center
BIAR	Biometric Intelligence Analysis Report
Bio API	Biometric Application Programming Interface
BIR	Biometric Information Record
BIR	Biometric Intelligence Resource
BISA	Biometric Identification System for Access
BMO	Biometric Management Office
BSWG	Biometric Standards Working Group
BTF	Biometric Task Force
CAC	Common Access Card
CBA	Capabilities Based Assessment
CBEFF	Common Biometric Exchange File Format
CBEFF	Common Biometric Exchange Formats Framework
CE	Communications Equipment
CENTCOM	Central Command
CJIS	Criminal Justice Information Services
CMC	Cumulative Match Characteristic
CMR	Cumulative Match Rate
CONOPS	Concept of Operations

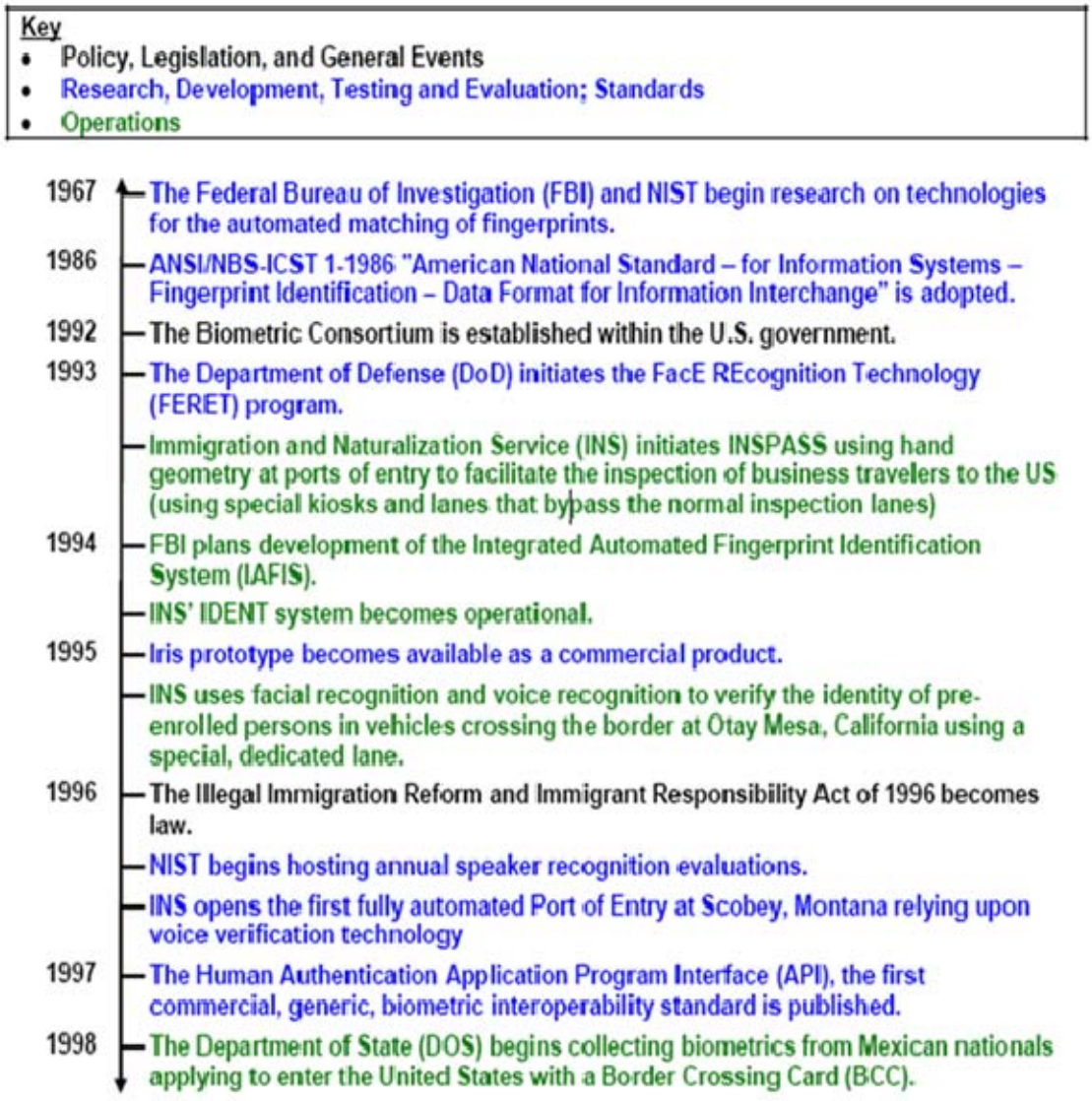
Acronyms

DBEKS	DoD Biometric Expert Knowledgebase System
DBIDS	Defense Biometric Identification System
DET	Detection Error Trade off
DMDC	Defense Manpower Data Center
DNA	Deoxyribonucleic Acid
DoD	Department of Defense
DPI	Dots Per Inch
DRS	Detainee Reporting System
EBTS	Electronic Biometric Transmission Specification
EFTS	Electronic Fingerprint Transmission Specification
EMIO	Expanded Maritime Interdiction Operations (NAVY)
FAR	False Acceptance Rate
FBI	Federal Bureau of Investigation
FHA	Foreign Humanitarian Assistance
FMR	False Match Rate
FNMR	False Non Match Rate
FOUO	For Official Use Only
FP	Force Protection
FpVTE	Fingerprint Vendor Technology Evaluation
FRR	False Rejection Rate
FRVT	Face Recognition Vendor Test
FTA	Failure To Acquire
FTE	Failure To Enroll
GMM	Gaussian Mixture Model
HD	Hamming Distance
HMM	Hidden Markov Model
IAFIS	Integrated Automated Fingerprint Identification System

Acronyms

IBDD	Integrated Biometric Data Dictionary
IDS_MD	Identity Dominance System - Maritime Domain
INCITS	International Committee for Information Technology Standards
ISO	International Organization for Standardization
JPEG	Joint Photographic Experts Group
JTC	Joint Technical Committee
LDM	Logical Data Model
LEP	Locally Employed Personnel
NGIC	National Ground Intelligence Center
NIST	National Institute of Standards and Technology
NSTC	National Science and Technology Council
ORCON	Dessemination & Extraction of Information Controlled by Originator
POI	Person(s) of Interest
PPI	Pixels Per Inch
RAPID	Real-time Automated Personnel Identification System
RFS	Ready For Staffing
ROC	Receiver Operating Characteristics
SCI	Sensitive Compartmented Information
SME	Subject Matter Expert
SWGFAST	Scientific Working Group on Friction Ridge Analysis, Study and Technology
TS	Top Secret
WSQ	Wavelet Scalar Quantization
XML	Extensible Markup Language

APPENDIX C — GENERAL TIMELINE OF FEDERAL GOVERNMENT BIOMETRIC ACTIVITIES




1999
FBI's IAFIS major components become operational.
2000
The first Face Recognition Vendor Test (FRVT 2000) is held.
DoD establishes its Biometrics Management Office (BMO) and Biometrics Fusion Center (BFC).
The Visa Waiver Program Act of 2000 becomes law.
The Defense Advance Research Projects Agency (DARPA) begins the Human Identification at a Distance (HumanID) Program.
The Biometric Application Programming Interface (BioAPI) specification is released.
2001
The terrorist attacks of September 11, 2001 occur.
FAA establishes Aviation Security Biometrics Working Group.
INCITS establishes M1 Technical Committee on Biometrics.
The USA PATRIOT Act becomes law.
The Center for Identification Technology Research (CITeR) begins operation as a National Science Foundation Industry/University Cooperative Research Center.
2002
The Enhanced Border Security and Visa Entry Reform Act becomes law.
The ISO/IEC SC 37 standards subcommittee on biometrics is established.
The Maritime Transportation Security Act becomes law, establishing the Transportation Worker Identification Credential (TWIC).
FRVT 2002 is held.
The E-Government Act of 2002 becomes law.
2003
DOS begins collecting biometrics from visa applicants through the BioVisa program.
The National Science and Technology Council charters a Subcommittee on Biometrics to coordinate biometrics research and development (R&D), policy, outreach, and international collaboration across the federal government.
ICAO adopts blueprint to integrate biometrics into machine-readable travel documents.
The Department of Justice (DOJ), DOS and NIST submit joint Patriot Act report to Congress on "Use of Technology Standards and Interoperable Databases with Machine-Readable, Tamper-Resistant Travel Documents"
Testing for the Fingerprint Vendor Technology Evaluation (FpVTE 2003) begins.
NIST begins Proprietary Fingerprint Template (PFT) testing.
Homeland Security Presidential Directive (HSPD) 6 establishes the Terrorist Screening Center.
2004
HSPD-11 establishes a coordinated and comprehensive approach to terrorist-related screening.
HSPD-12 calls for standard, government-wide personal identification verification (PIV) credentials for all federal employees and contractors.
Face Recognition Grand Challenge begins.
International Meeting of Biometrics Experts held.
DHS' US-VISIT program begins collecting biometrics from international visitors at all international air, sea, and land border ports of entry.
AirNexus kickoff – facilitated travel program operated jointly with the Government of Canada using iris verification at kiosks for pre-enrolled travelers

- Slap Fingerprint Segmentation Evaluation 2004 (SlapSeg04).
- DoD's IAFIS-compatible database, Automated Biometric Identification System (ABIS), becomes operational.
- The fingerprint Minutiae Interoperability Exchange 2004 (MINEX 04) tests begin.
- The Intelligence Reform and Terrorism Prevention Act becomes law.
- DHS and NIST initiate a program to develop human computer interaction (HCI) guidelines and standards for biometric systems.
- The first statewide automated palm print databases in the United States are deployed in California, Connecticut, and Rhode Island.
- The first Common Biometric Exchange Formats Framework (CBEFF) ANSI standard is published.
- NIST Fingerprint Image Quality assessment tool is released.

2005

- NIST issues standards for federally mandated, government-wide PIV cards.
- NIST hosts the 10-Print Capture Scanner & Software Requirements Workshop.
- The Iris Challenge Evaluation 2005 (ICE 2005) Program is held.
- The European Commission hosts a "Workshop on Ethical and Social Implications of Biometric Identification Technology: Toward an International Approach."

2006

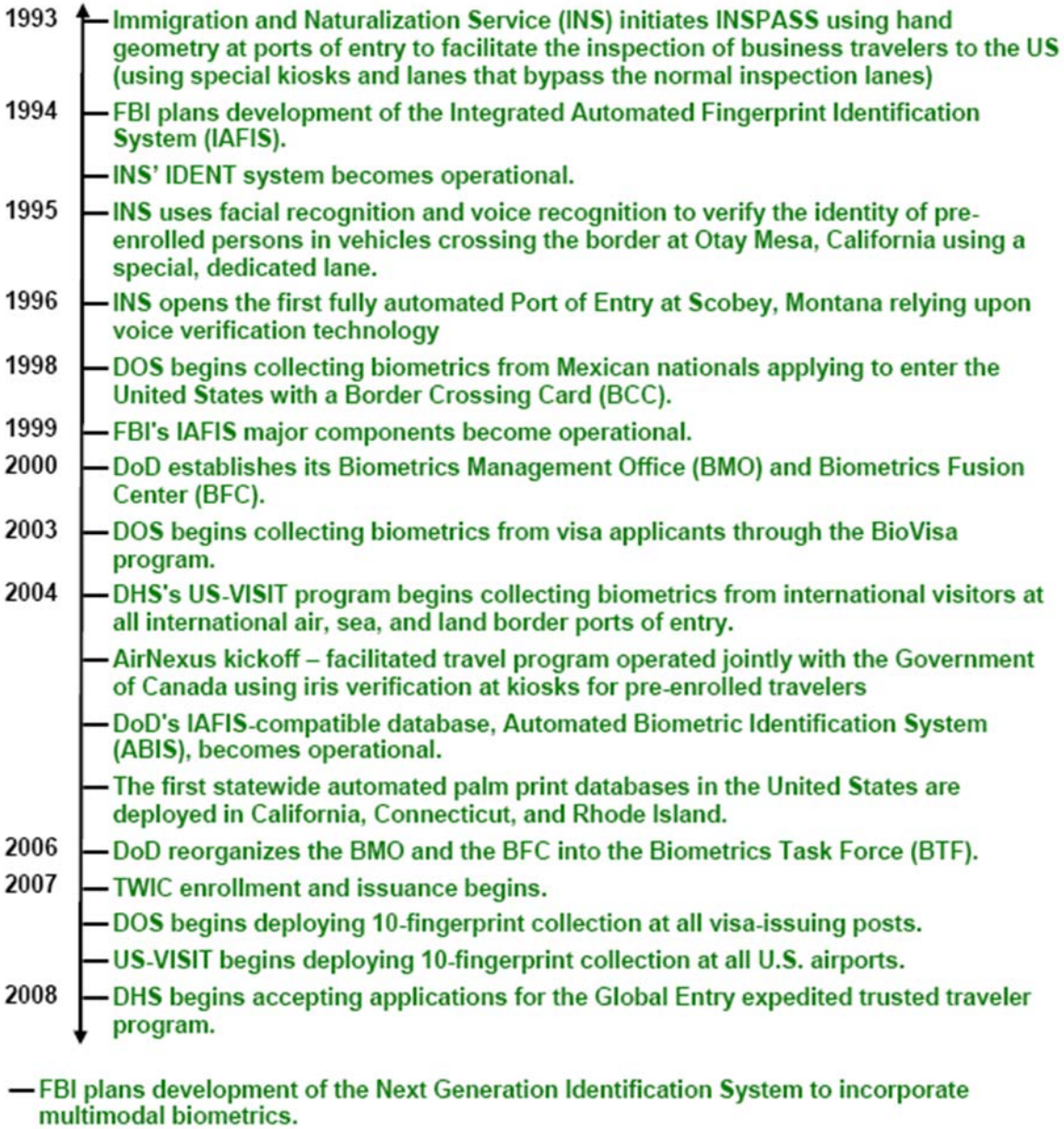
- DoD reorganizes the BMO and the BFC into the Biometrics Task Force (BTF).
- FRVT 2006 is held.
- First international *NIST Biometric Quality Workshop* is held.
- Defense Science Board launches Task Force to study biometrics in the DoD.
- DHS hosts the 10-Print Capture User Group Industry Day.
- NIST holds the Latent Fingerprint Testing Workshop.
- Agencies, working through the NSTC, begin the process of designing government-wide biometric system interoperability.
- The President approves the *National Implementation Plan for the War on Terror.*
- www.biometrics.gov is launched.
- *The National Biometrics Challenge* is issued.
- ICE 2006 is held.
- The United States hosts the "International Conference on Biometrics and Ethics"

2007

- Agencies, working through the NSTC and National Counterterrorism Center, begin collaboration to improve the coordination of biometric activities to support efforts against known and suspected terrorists.
- TWIC Enrollment and Issuance begins.
- Technology demonstrations for the Fast Capture Rolled-Equivalent Finger/Palm Print Initiative begin.
- NSTC expands the focus of its existing biometrics subcommittee, creating the NSTC Subcommittee on Biometrics and Identity Management.
- NIST conducts Phase I of the Evaluation of Latent Fingerprint Technologies (ELFT).
- ANSI/NIST-ITL 1-2007 – Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information – Part 1 is adopted.
- NIST conducts MINEX II (Fingerprint Match on Card).
- DHS *Privacy Technology Implementation Guide* is issued.
- *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards* is issued.


NIST releases public domain build instructions for the Multimodal Biometric Application Resource Kit (MBARK).
DOS begins deploying 10-fingerprint collection at all visa-issuing posts.
US-VISIT begins deploying 10-fingerprint collection at all U.S. airports.
2008
The NSTC Task Force on Identity Management is chartered.
The Multiple Biometric Grand Challenge (MBGC) begins.
DHS begins accepting applications for the Global Entry expedited trusted traveler program.
FBI plans development of the Next Generation Identification System to incorporate multimodal biometrics.
NSTC Registry of USG Recommended Biometric Standards is issued.
The President issues NSPD-59/HSPD-24: Biometrics for Identification and Screening to Enhance National Security.
The International Workshop on Usability and Biometrics is held.
ANSI/NIST-ITL 2-2008 – XML Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information – Part 2 is adopted.

APPENDIX D — BIOMETRICS OPERATIONS TIMELINE



THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Biometrics, NSTC Subcommittee on. The National Biometrics Challenge. Point paper. Washington: Executive Office of the President of the United States, 2006.

Blackburn, James. NSTC Subcommitte on Biometrics and Identity Management. PPT Presentation. Washington: Executive Office of the President, 2008.

Council, National Science and Technology. Identity Management Task Force Report 2008. Washington, DC, 2008.

———. ñSubcommittee Overview.” 2009. Biometrics.gov. February 10, 2009 <http://www.biometrics.gov/nstc/Overview.aspx>.

Defense, Deputy Secretary of. “Department of Defense Biometrics.” Department of Defense Directive 8521.01E. Washington: Department of Defense, February 21, 2008.

———. ñDirective-Type Memorandum (DTM) 08-006 — DoD Implementation of Homeland Security Presidential Directive — 12 (HSPD-12).ò Washington: Department of Defense, November 26, 2008.

Dray, James. National Science and Technology Council Task Force on Identity Management. PPT Presentation. Washington: Executive Office of the President of the United States, 2008.

House, Office of the White. “NSTC Executive Order 12881.” November 23, 1993. National Science & Technology Council. February 10, 2009 <http://www.ostp.gov/cs/nstc/executive_order>.

Kim, Dr. Richard. ñBio-Pen Applications.ò Tempe: DynaSig Corporation, May 27, 2008.

———. “Bio-Pen Presentation.” Tempe: DynaSig Corporation, May 3, 2007.

———. “Bio-Pen White Paper: Security Features.” Tempe: DynaSig Corporation, 2005.

National Biometric Security Project. Biometric Technology Application Manual: Volume I Biometrics Basics. Public education. Washington: National Biometric Security Project, 2005.

National Science & Technology Council. BIOMETRICS in Government POST-9/11. Research and Policy Guidance. Washington: Executive Office of the President, 2008.

NSTC — Face. Face Recognition. Washington, August 7, 2006.

NSTC — Fingerprint. Fingerprint Recognition. Washington, August 7, 2006.

NSTC — Iris. Iris Recognition. Washington, August 7, 2006.

NSTC — Signature. Dynamic Signature. Washington, August 7, 2006.

NSTC — Speaker. Speaker Recognition. Washington, August 7, 2006.

(P&R), Under Secretary of Defense. "DoD Personnel Identity Protection (PIP) Program." Department of Defense Directive 1000.25. Washington: Department of Defense, April 23, 2007.

President, Executive Office of the. "About NSTC." 2009. National Science & Technology Council. February 10, 2009 <http://www.ostp.gov/cs/nstc/about>.

Security, Department of Homeland. "Privacy Office — Privacy Impact Assessments (PIA)." Department of Homeland Security. February 11, 2009 <http://www.dhs.gov/xinfoshare/publications/editorial_0511.shtm>.

Technology, National Institute of Standards and. "Federal Information Processing Standards Publication." Personal Identity Verification (PIV) of Federal Employees and Contractors. Gaithersburg: Department of Commerce, March 2006.

TF on Biometrics, Defense Science Board. "Report of the Defense Science Board Task Force on Defense Biometrics." Washington: USD (AT&L), March 2007.

White House, Office of the. "Homeland Security Presidential Directive 12." August 27, 2004. Department of Homeland Security. January 15, 2009 <http://www.dhs.gov/xabout/laws/gc_1214594853475.shtm>.

———. "Homeland Security Presidential Directive 24." June 5, 2008. Department of Homeland Security. January 15, 2009 <http://www.dhs.gov/xabout/laws/gc_1219257118875.shtm>.

———. "Homeland Security Presidential Directive 6." September 16, 2003. Department of Homeland Security. January 15, 2008 <http://www.dhs.gov/xabout/laws/gc_1214594853475.shtm>.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Jim F. Ehlert
   Naval Postgraduate School
   Monterey, California

4. Dr. Pat Sankar
   Naval Postgraduate School
   Monterey, California

5. Edward Fisher
   Naval Postgraduate School
   Monterey, California

6. Dr. Richard Kim
   DynaSig Corporation
   Phoenix, Arizona